নিরাপদ প্রযুক্তি

Safer net

(প্রথম এডিশন)

কৃতজ্ঞতায়

সেফার নেট টিম

সূচীপত্র

নেট সিকিউরিটির ব্যপারে মৌলিক ধারনা

প্রথম অধ্যায়

আমরা সিকিউরিটির ব্যপারে শুরু থেকে সব বিষয় গুলো আলোচনা করব। যাতে করে নিত্ব-নতুন যে বিষয়গুলো প্রতিনিয়ত আমাদের সামনে আসছে তার আলোকে সিকিউরিটির ব্যপারে অবগত করা যায়। এটা ধারাবাহিক ভাবে সময়ে সময়ে আপনাদের কে জানাব ইনশাআল্লাহ । আজ কিছু উপকারী বিষয় আপনাদের সামনে আলোচনা করব যেগুলো সিকিউরিটি এবং প্রাইভেসির প্রাথমিক ধারনা বলা যায়।

বর্তমানে আমরিকার গোপন এজেন্সি "এন,এস,আই," ইন্টারনেটের মাধ্যমে সকল দেশের উপর বড় ধরনের নজরদারি করছে। আজ থেকে চার বছর পুর্বে 'এড ওয়ার্ড স্নোডেন' যে এন,এস,আইতে কন্ট্রাক্টর হিসেবে কাজ করত, সেখান থেকে সে তাদের সমস্ত গোপন তথ্য সংগ্রহ করেছিল। এবং তাদের নজরদারির কথা পুরো দুনিয়ার সামনে প্রকাশ করেছিল যে, কোন মাধ্যমে তারা নজরদারি করে যাচ্ছে।

এই গোপন তথ্যে সে একটি প্রোগ্রামের নাম উল্লেখ করেছে যার নাম ছিল প্রিজম (prism)। এই প্রোগ্রামে আন্ডারে ৯টি বড় বড় কম্পানি তাদের ডাটা এন এস আই কে প্রদান করে থেকে। তাদের মধ্য থেকে এ সকল কম্পানি উল্লেখ যোগ্যঃ-

১/ মাইক্রোসফট ২/ গোগল ৩/ ফেসবুক ৪/ ইয়াহু ৫/ অ্যাপল ৬/ পালটাক ৭/ ইউটিউব ৮/ স্কাইপ ৯/ আই ও এল

এই কম্পানি গুলো নিজেদের বিভিন্ন এপ ও সোর্সের মাধ্যমে নজরদারী করে যাচ্ছে। যেমন: গোগল সার্চ ইঞ্জিন, গোগল প্লে স্টোর, জিমেইল ইত্যাদি,

কিছু কম্পানি তো একে অন্যের সাথে মিশে গেছে। এটা জেনে রাখুন, গোগল, মাইক্রোসফট, অ্যাপেল এবং ফেসবুক এর মাঝে এক ধরনের যুদ্ধ চলছে। কে কার থেকে বেশি ব্যবহারকারীদের তথ্য নিতে পারে। এবং তারা তার বিভিন্ন পদ্ধতি ও বের করেছে। এবং এই সকল তথ্য, মেসেজ, মেইল ইত্যাদি এন,এস,আইকে প্রদান করে থাকে।

বর্তমানে গোগল, ফেসবুক ব্যবহারকারীদের সব থেকে বেশি তথ্য গ্রহণ করে, এবং তার বিভিন্ন পদ্ধতিও আপনারা প্রতিনিয়ত পত্রপত্রিকায় দেখতে পারছেন। গুগল এবং ফেসবুকে লগইন করে যদি আপনি ব্রাউজের মাধ্যমে কিছু সার্চ করেন, তখন সে আপনার ব্যপারে এটা জানতে পারবে যে আপনি কি চাচ্ছেন আর এই ডাটা সে সংরক্ষিত রাখে। এমনিতে মেইল, মেসেজ দেখা ও সংরক্ষণ তো অবশ্যই করে। সাথে সাথে সে তার চেয়েও কয়েকগুন বেশি আমাদের নজরদারি করছে।

যে যে ওয়েবসাইট খুলা হয়েছে, যদি ব্রাউজারের কুকিস এবং হিস্টরি সব সময় পরিস্কার না করে তাহলে তাদের কাছে এই তথ্য চলে যায়। এ থেকে বাচার জন্যে এই সব সার্ভিস ব্যবহার ছেড়ে দেয়া ছাড়া আর কোন উপায় নেই। আমরা এর বিকল্পগুলো ব্যবহার করতে পারি ইনশাআল্লাহ।

এখন এখানে আরেকটি কথা যা অধিকাংশ সাথিরা জিজ্ঞাসা করে থাকে। যে এই দেশেও কি এগুলো ব্যবহার করার দ্বারা আমাদের মেইল এবং মেসেজ ট্র্যাক করা হয়? অর্থাৎ বাংলাদেশের এজেন্সি এটা ধরতে পারে? স্বরণ রাখবেন যে, সরকারের কাছে এমন কোন যন্ত্র নেই যার দ্বারা মেইল এবং মেসেজ ট্রাস করতে পারবে। কেননা জিমেইল হোক বা ফেসবুক মেসেঞ্জার, এখন উভয়টাই ইনক্রিপ্টেড ট্রান্সমিটার ব্যবহার করে থাকে। অর্থাৎ মাঝখান থেকে কোন হ্যকার বা এজেন্সি ট্র্যাক করতে পারেনা। কিন্তু এখানে এই কথা অবশ্যই খেয়াল রাখবেন যে, গোগল এবং ফেসবুক প্রত্যেক দেশের ত্বাগুতী সরকারকে পুর্ণ সহযোগীতা করে। এবং এটা তাদের প্রাইভেসী নিয়মনীতির অংশ যে তারা এই ডাটা প্রশাসন চাওয়ার সাথে সাথে তাদের সাথে শেয়ার করে থাকে।

এটা আপনার উপর নির্ভর করে যে আপনি সরকারের জন্য কতটুকু গুরুত্বপূর্ণ। প্রতি বছর ফেসবুক এবং গোগল মিনিমাম এক হাজার ব্যবহারকারীর ডাটা সরকারের কাছে হস্তান্তর করে থাকে। এখন আপনি দেখুন যে আপনি নেটের জগতে কতটুকু গুরুত্বপূর্ন। আপনি কি সেই **১** হাজার বা দেড় হাজারের রেঞ্জের ভিতরে পরবেন?

সতর্কতা এর ভিতরেই যে যোগাযোগ এর জন্য ফেসবুক ও জিমেইল একদম ব্যবহার না করা।

দ্বিতীয় অধ্যায়

এই অধ্যায়ে আমরা সে সকল দেশ সমপর্কে আলোচনা করব যারা পুরা বিশ্বে নজরদারী ও তত্বাবধারন করে যাচ্ছে। এবং তারা পরস্পরে গোপন বিষয় সমূহ শেয়ার করে থাকে।

স্নোডেন ঐ পাঁচ দেশের আলোচনা করেছেন যে পাঁচ দেশের বিভিন্ন এজেন্সি পরস্পরে তথ্য শেয়ার করে থাকে। এবং এই পাঁচটি দেশকে ইন্টারনেট প্রাইভেসির শত্রু মনে করা হয়। এই পাঁচ দেশকে Five Eyes অর্থাৎ পাঁচ চোখ এর নাম দেয়া হয়েছে। দেশগুলো হল:-

১/ আমিরিকা ২/ ব্রিটেন ৩/ কানাডা ৪/ অষ্ট্রেলিয়া ৫/ নিউজিল্যান্ড এবং আরেক সহযোগী হল ইসরাইল।

উল্লেখিত পাঁচ দেশের পরস্পরে একতা এবং বন্ধুত্ব রয়েছে। এবং ইন্টিলিজেন্স শেয়ার হয়ে থাকে। এরপর তাদের পরস্পরে আরেকটা চুক্তি স্বাক্ষরিত হয়, যাকে সিকিউরিটি বিশেষজ্ঞরা Fourteen Eyes অর্থাৎ চৌদ্দ চোখ নাম দিয়েছে। যার মধ্যে পুর্বে উল্লেখ করা ছয়টি নাম ছাড়া ও আরো কিছু দেশের নাম শামিল হয়েছে।

৭/ ইটালি ৮/ স্পেন ৯/ সুইডেন ১০/ ডেনমার্ক ১১/ বেলজিয়াম ১২/ ফ্রান্স ১৩/ নেদারল্যান্ড ১৪/ নরওয়ে ১৫/ জার্মানি

এই চুক্তি sigint seniors Europe নামে পরিচিত। এখানে তাদের এন্টিলিজেন্স শেয়ারিং হয় সন্ত্রাসের বিরুদ্ধে। কিন্তু ছাড়াও আরো কিছু দেশ রয়েছে যারা এর মধ্যে শামিল। সিংগাপুর, উত্তর কোরিয়া, জাপান এবং ব্রেটেনের অধিনস্ত কিছু এলাকা।

এই লিষ্ট উল্লেখ করার উদ্দেশ্য হল যে, যে পাঁচ + এক দেশের কথা উল্লেখ করা হল, ঐসব দেশের সব মাধ্যম একেবারেই ব্যবহার না করা। কেননা এই সব দেশ গুলোকে অনলাইন প্রাইভেসির শত্রু মনে করা হয়। এরা কোন কম্পানিকেই স্বাধিন থাকতে দেয়না। বরং তাদের দেশের কম্পানিগুলোর ব্যবহারকারীদের সমস্ত তথ্য রাখে। এবং এই দেশগুলো তথ্য ও ডাটা একে অন্যের সাথে শেয়ার করে।

তাদের সোর্সের মধ্যে থেকে কিছু এখানে উল্লেখ করা হল:-

Email – Gmail, Yahoo, Hotmail ইত্যাদি
cloud storage - Dropbox, Google Drive ইত্যাদি
Messenger – Whats app, Facebook, Google Alo, Skype ইত্যাদি।
VPN – IP venish, Hide me s, Hotspot shelid ইত্যাদি।
Social Media - Facebook, Google plus, Twiter ইত্যাদি।
Operating system - windows, android, IOS, mac ইত্যাদি।
Web hosting এবং এছাড়াও আরো অন্যান্য মাধ্যম।

এরা ছাড়া আরো যে ১২ দেশের আলোচনা করা হয়েছে তাদের সোর্স সতর্কতার সাথে ব্যবহার করা উচিৎ। এই সকল দেশ যদিও ব্যাপকভাবে ইন্টিলিজেন্স শেয়ার করেনা, কিন্তু কিছু তো হয়ই। আর বিশেষ ভাবে মুজাহিদিনের বিরুদ্ধে তো অবশ্যই। কিন্তু তাদের মধ্যে কিছু আছে সাধারণ জনগনের প্রাইভেসী লক্ষ করে এবং সেই পরিনাম ইন্টারনেটের শত্রু মনে করা হয় না। এবং কম্পানিকে বেশি চাপ প্রয়োগ করা হয় না। যেমন জার্মানি আছে এই জাতীয় দেশের সোর্স সতর্কতার সহিত ব্যবহার করা যেতে পারে।

তৃতিয় অধ্যায়

এই অধ্যায়ে আপনাদের সামনে তুলে ধরার চেষ্টা করব যে, NSI আরো কোন মাধ্যমেগুলো দ্বারা ইন্টারনেটে লোকদের নজরদারী করে যাচ্ছে। এডওয়ার্ড স্নোডেন এখানে কিছু প্রোগ্রামের কথা উল্লেখ করে ছিলেন, যার মধ্যে হচ্ছেঃ

XKeyscore - এই প্রগ্রাম পুরো বিশ্বে ব্যপকভাবে ইন্টারনেটের নজরদারির জন্য বানিয়েছে। যার জন্যে ১৫০ দেশের বিভিন্ন জায়গায় ৭০০ বড় বড় সার্ভার স্থাপন করেছে যা সকল ইন্টারনেট ট্রাফিককে স্টোর করে থাকে। এর মাধ্যমে একজন সাধারণ এন এস আই কর্মকর্তা যে কারো মেইল পড়তে পারে। এবং যে কারো নজরদারী করতে পারে যে; সে আজ কি কি করছে, কোন কোন ওয়েব সাইট খুলেছে। সে আপনার ট্রাফিককে শুধু দেখেই না বরং এই ডাটা তার কাছে সংরক্ষিত থাকে। কিছু দিনের জন্য ভিতর সে কারো ডাটা দেখতে চাইলে সে তা দেখতে পারে।

রিপোর্ট অনুযায়ী কয়েকটি সার্ভার ভারত ও পাকিস্তানে আছে। এই প্রোগ্রাম অত্যন্ত ব্যপক ও বড় মাপের সিস্টেম যার মধ্যে আরো কয়েকটি প্রোগ্রাম রয়েছে। যার মধ্য থেকে একটি হলঃ-

Tempora - এটা বৃটেনের ইন্টেলিজেন্স এজেন্সি "গভর্নমেন্ট কমিউনিকেশন হেডকোয়াটার " এর প্রোগ্রাম। যার অধিনে সকল ধরনের ফাইবার অপটিক্যাল ইন্টারনেট ট্রাফিককে নিজের কাছে সংরক্ষণ করে নেয়। যাতে পরবর্তিতে যখন কারো ব্যপারে দেখতে হয় তখন ঐ সার্ভার থেকে দেখা যায়। পুরো বিশ্বে ইন্টারনেট ফাইবার অপটিক্স কেবল এর মাধ্যমেই ছড়িয়ে আছে। বৃটেনের ইন্টেলিজেন্স এজেন্সি এই তথ্য গুলো এন এস আই এর সাথে শেয়ার করে থাকে। এবং তাকে এই আশ্বাস দিয়ে রেখেছে।

ঐ প্রগ্রামগুলোর এক বৈশিষ্ট এটাও রয়েছে, যে তার মধ্যে অধিকাংশ ভাষার অনুবাদ নিজে নিজেই হয়ে যায়। তাদের অন্য কোন অনুবাদকের প্রয়োজন পড়েনা। রিপোর্ট অনুযায়ী সে পুরো বিশ্বের এক মাসের ট্রাকিং তথ্য নিজের কাছে জমা রাখতে পারে। এবং সে একাই এক্স কি স্কোর চেয়ে বেশি তথ্য জমা রাখতে পারে। আরেকটা প্রোগ্রামের নাম হলঃ-

ECHELON - বড় দেশগুলো এটা ব্যবহার করে। এই প্রগ্রামের কাজ হল অন্যান্য দেশ গুলোর সেটেলাইট নজরদারি করা। তাদের ফোন কল ট্রেস করা এবং মেসেজ ইত্যাদি দেখা এই ডাটা আবার এক্স কি স্কোরের সার্ভারে জমা হয়ে যায়।

এছাড়া এন এস আই এর নজরদারির আরো অনেক প্রোগ্রাম রয়েছে সব গুলো নিয়ে আলোচনা করা সম্ভব না। এই জন্যই তো গুগল বলেছিল যে, আমাদের এটা জানা আছে যে লোকেরা কতবার নিজেদের মোবাইলের লক খুলে।

এই কথা গুলোকে সংক্ষিপ্ত ভাবে বলার উদ্দেশ্য ছিল, ইন্টারনেটে যেকোন জিনিষই আপনি করেন না কেন তা NSI এর নজরদারির বাইরে নয়। বাকি কল ট্রেস ও মেসেজ ট্রেস করা তো বাংলাদেশেও করে থাকে, এটা তাদের জন্য কোন বড় কিছু না। ইন্টারনেটে যতক্ষন পর্যন্ত ইনক্রিপ্ট ট্রাফিক ব্যবহার না করবেন ততক্ষণ পর্যন্ত আপনার সকল খবরা খবর তাদের কাছে থাকে, আপনি কি কি দেখছেন, ইন্টারনেটে আরো কি কি জিনিষ ডাউনলোড করছেন। তবে ইন্টারনেট থেকে ইনক্রিপ্ট করা তথ্য বা কলের ব্যপারে গোয়েন্দা সংস্থা সহ কেহই জানতে পারে না। এই জন্য আমরা বারংবার ইনক্রিপ্ট ট্রাফিকের জন্য কোন ভাল "VPN" এর ব্যবহারের পরামর্শ দেই।

গুরুত্বপূর্ন ব্যপার হচ্ছে; ইন্টারনেটে সবার ইনফর্মেশন চেক করা হয় না। বরং যে সন্দেহে থাকে বা নজরে পড়ে যায় তারটা দেখা হয়। অধিকাংশ লোক নজরে পড়ে অসতর্কতার কারনে। এই জন্য সতর্কতার খাতিরে ভাল কোন VPN ব্যবহার করবেন। যাতে আপনার তথ্য সব ইনক্রিপ্ট করা থাকে এবং আপনি শত্রুর দৃষ্টি থেকে নিরাপদ থাকেন।

Encryption এর আলোচনা

Encryption এটাকে বাংলাতে বলা হয় গোপন করা। তবে যেহুতু আমাদের এখানের সর্ব সাধারণ ইংরেজি শব্দ ব্যবহারে অধিক অভ্যস্ত তাই আমরা আমাদের আলোচনায় ইংরেজি শব্দটাই ব্যবহার করব।

Encryption বলা হয় গোপনীয়তার জন্য তথ্যাবলীকে এমন ভাবে incode করা যাতে মূল বার্তা বিশেষ কিছু ব্যক্তিই বুঝতে সক্ষম হন (অন্য কেহ নয়)। Encryption কোন ব্যক্তিকে বার্তা বা বিষয় বস্তু পর্যন্ত পৌছতে বাধা দিতে সক্ষম নয় । তবে যার এই বার্তার কোডিং জানা নাই সে এই বার্তা পাঠ করে কিছুই বুঝবে না। এই বার্তা বুঝার জন্য অপর ব্যক্তিকে অপরিহার্য ভাবে এই বার্তা বুঝার পদ্বতিও জানতে হবে।

Encryption গোপনে চিঠি প্রেরনের বহু পুরাতন পদ্ধতি। আগের যুগে চিঠি পত্র সাধারণত শব্দের (text) মাধ্যমে লেখা হত। এজন্য Encryption এর পরেও চিঠি শব্দের আকৃতিতেই রয়ে যেত। আধুনিক যুগে বিশেষ করে কম্পিউটার আবিস্কারের পর শব্দ, অডিও, ভিডিও এবং অন্যান্য ডেটায় Encryption লাগিয়ে বার্তা নিরাপদ করা যায়।

Encryption নিজেও করা যায় কম্পিউটারের সাহায্যে ও করা যায়। নিজে করার সর্ব প্রাচীন পদ্ধতি হলো: আপনি একটি অক্ষরের স্থানে অন্য আরেকটি অক্ষর ব্যবহার করবেন। উদাহরণত cat শব্দটির ক্ষেত্রে আপনি Cএর স্থানে G, A এর স্থানে K. Tএর স্থানে R লিখবেন। ফলে শব্দ CAT কে যখন Encryption করা হলো সেটা GKR রুপ ধারণ করল । তখন বার্তা প্রেরক GKR লিখে মেসেজ করবে আর বার্তা প্রাপক সেটা ঠিক করে CAT করে নিবে । এমনি ভাবে সমস্ত অক্ষরগুলিকে আলাদা আলাদা ভাবে শৃংখলাবদ্ধ করে দিবেন,

যেখানে A লিখতে চান সেখানে K লিখবেন আর যাকে মেসেজ করবেন তাকে পুর্বে থেকেই জানিয়ে রাখতে হবে কোন অক্ষরের স্থানে কোন আক্ষরটি হবে। সে সেই অনুযায়ী অক্ষর গুলো ঠিক করে মেসেজ টি পড়বে ।

এই পদ্বতি প্রথম বিশ্ব যুদ্ধে ব্যবহৃত হয়েছিল তার পর দ্বিতীয় বিশ্ব যুদ্বে মেশিনের সাহায্যে Encryption করা হত. এখন বর্তমানে কম্পিওটারের সাহায্যে Encryption করা হয়. কম্পিওটারের মাধ্যমে করা Encryption বহুত শক্তিশালী ও নিরাপদ হয় যা সহজে ভান্গা যায় না। এই লক্ষেই Encryption এলগরিদম ব্যবহার করা হয়। ইদানিং বিভিন্ন ধরণের এলগরিদম ব্যবহার হচ্ছে।

Encryption এর মৌলিক উদ্দেশ্য হলো আপনি যাকে মেসেজ অথবা অন্য কিছু পাঠাতে চান তা অন্য কেহ যেন জানতে না পারে কী পাঠাচ্ছেন। যেমনটা অতিত কালে আমরা যখন কারো নিকট চিঠি পাঠাতাম তখন পথিমধ্যে অন্য কেহ তা পড়ে ফেলার একটা আশংকা থাকত। তেমনি ভাবে আমরা যখন ল্যান্ড লাইনের মাধ্যমে কথা বলি তখন মাঝে মধ্যে একচেন্জ কর্মকর্তাদের আওয়াজ শোনা যায় যার ফলে আমরা বুঝতে পারি তারা আমাদের কথা শুনছে অথবা কখনো আমরা নিজেরাই চালাকি করে কোন কেবিনেটে টেলিফোন লাগিয়ে লোকদের কল ভয়েস শুনে থাকি ।

এমনি ভাবে বর্তমান প্রযুক্তির যুগেও এটা সম্ভব যে, আপনি ইন্টারনেটে যা কিছুই পাঠান বা ডাউনলোড করেন অথবা মেসেজ কিংবা কল করেন, যদি তা Encrypted করা না থাকে, তৃতীয় ব্যক্তি জানতে পারবে যে পাঠানো জিনিসটা কি ছিল। ইন্টারনেটে ডেটাগুলো প্যাকেটের আকৃতিতে থাকে যা বিভিন্ন নেটওয়ার্কিং সফটওয়্যাররের মাধ্যমে দেখা যায় যে এই প্যাকেটের মধ্যে কী আছে। ইন্টারনেটের মধ্যস্হতা কারী প্রতিষ্ঠান এটা দেখতে পারেন। ধরুন আপনার ISP অর্থাৎ ইন্টারনেট সার্ভিস প্রভাইডার সীম কম্পানী যারা আপনাকে ইন্টারনেট সুবিধা সরবরাহ করছেন অথবা আপনি যদি Wi-Fi ব্যবহার করে থাকেন তাহলে এই রাউডারের এক্সেস যার কাছে থাকবে সেও দেখতে পারবে।

এটা ছাড়াও মধ্যস্থতাকারী আরো কিছু পয়েন্ট রয়েছে। একটি উদাহরণ দিচ্ছি, ধরুন আপনি এমন একটি অ্যাপ ব্যবহার করছেন যা মেসেজকে Encrypt করে পাঠায় না তাহলে এখন আপনার wifi রাউডার. আপনার ISP ও যেখান থেকে ISP নেট সংযোগ নিয়েছে এবং এই অ্যাপের কোম্পানী সবার কাছে এই ডেটা পৌছে যাচ্ছে আর এরা সবাই আপনার মেসেজ

পড়তে সক্ষম। এটা এক দিকের কথা। দ্বিতীয় দিকে ও এমনটাই হবে অর্থাৎ কম্পানি থেকে স্যাটেলাইট সেখান থেকে সেটালাইটের সামনে বস থাকা ব্যক্তি, ও যার কাছে মেসেজ পাঠানো হয়েছে তার ISP এই মেসেজ পড়তে সক্ষম।

এটা শুধু একটা উদাহরণ, বর্তমানে প্রায় সব মেসেন্জার অ্যাপ গুলোই Encryption ব্যবহার করে থাকে কেহ এন্ড টু এন্ড অর্থাৎ এক ব্যক্তি থেকে দ্বীতীয় ব্যক্তি পর্যন্ত Encrypted থাকে মধ্যখানে কোথায়ও decrypt হয়না। আর কিছু শুধু এক এন্ড থেকে কম্পানির সার্ভার পর্যন্ত তারপর কম্পানি সার্ভার থেকে সামনের ব্যক্তি পর্যন্ত Encrypted থাকে অর্থাৎ কম্পানি নিজ সার্ভারে এটা De crypt করে। টেলিগ্রামের সাধারণ নরমাল চ্যাট এটার উদাহরণ।

যোগাযোগ মাধ্যমে ট্র্যাকিং ও নজরদারী

কোন ব্যক্তিকে নজরদারী করা ও ইন্টারনেটে তার কথা ও মেসেজ সংগ্রহের জন্যে মূল কাজ হচ্ছে তাকে ট্র্যাকিং করা। এই কথা প্রশিদ্ধ যে, কোন যোগাযোগ সিস্টেম পরিপূর্ণভাবে নিরাপদ বিবেচিত হয়, যখন সেই সিস্টেমটি কোডের মাধ্যমে ইনক্রিপ্টেড মেসেজ প্রেরকের থেকে নেটওয়ার্কিংয়ের মধ্য দিয়ে পূর্ণ নিরাপত্তার সাথে প্রাপকের কাছে পৌছাতে সক্ষম হয়। এবং তা সংযোগের সমস্ত পর্যায়ে (তার / বেতার)। তেনিভাবে কাউকে ট্র্যাকিং করা সম্ভব নয় যতক্ষন না ট্রেকিংয়ের উপযুক্ত নেটওয়ার্ক এর অধিনে আসবে এবং ডিভাইস বা সফটওয়্যার হ্যাকিং সম্ভব হবে। সেই সাথে হাজারো মানুষের মধ্যে টার্গেটকে নির্দিষ্ট করতে হবে।

একটা প্রশ্ন সবাই করেন, কীভাবে আমাদের ভয়েস কলের ট্রেকিং করা হয়? এবং কীভাবে মোবাইল ফোনের দ্বারা আমাদের যোগাযোগ ট্রেকিং করা হয়?

১/ ভয়েস কলের মধ্যস্থতা!

হ্যাকার ও পেশাদার হ্যাকারদের বিবেচনায় দ্বিতীয় প্রজন্ম ২G নেটওয়ার্ক নিরাপদ নয়। তাদের জন্য সাভাবিক কৌশলে এই নেটওয়ার্ক হ্যাক করা সম্ভব। তেমনিভাবে তাদের জন্য সম্ভব ক্ষতিকারক ডিভাইস ব্যবহার করার মাধ্যমে ৩G, 4G নেটওয়ার্ককে ২G দিকে ফিরিয়ে দেয়া। ফলে এভাবে এই নেটওয়ার্ককে হ্যাক করা সহজ হয়ে যায়।

২/ ইন্টারনেট যোগাযোগ ট্রেকিং

ইন্টারনেট ব্রাউজ করার জন্য সর্বদা ARP প্রটোকলের প্রয়োজন পরে। আর এই প্রটোকল ইন্টারনেট ব্যবহার করার সময় ওয়েব সাইটের লিংক তৈরি ও পরিচালনা করে থাকে। আর হ্যাকার ও পেশাদার ট্রেকারদের পক্ষে নেটের মাধ্যমে প্রেরিত Raw-material Packete তথ্যা ট্র্যাক করা, পরিবর্তন বা আটকিয়ে ফেলা সম্ভব।তেমনিভাবে Hotspots অথবা ওয়াইফাই এবং প্রাইভেট-পাবলিক প্রতিষ্ঠানগুলিতে বেতার নেটওয়ার্কগুলির মাধ্যমে প্রেরিত তথ্যাদি আটকানো সম্ভব। ঠিক তেমনি বেতার ট্রান্সমিশন এন্টেনা অথবা সুউচ্চ ভবনের উপরে যোগাযোগ টাওয়ারগুলি যোগাযোগও। এই কারনেই হ্যাকারের ইলেকট্রিক সিস্টেমের অধিনে কাজ করার জন্য ভিক্টিমের ডিভাইসের সংযোগ পরিবর্তন করে দেয়। ফলে যখন টার্গেট ব্যক্তি নিরাপদ ইন্টারনেট ব্রাউজকারী প্রটোকল HTTPS ব্যবহার করে তখন তারা সহজেই প্রটোকলকে অনিরাপদ সার্ফিং HTTP প্রটোকলে পরিবর্তন করে ফেলে।

৩/ পাবলিক টেলিফোন নেটওয়ার্কিং ট্র্যাকিং

সাভাবিকভাবে SMS ও ভয়েস কমিউনিকেশন ইনক্রিপ্টিড হয়ে স্থানান্তরিত হয় না! নিশ্চিতভাবে বলা যায় এগুলো অতিক্রম করে সাভাবিক যোগাযোগের নেটওয়ার্ক এর মধ্য দিয়ে। আর এভাবে ট্র্যাকিং ঝুকির সম্মুখীন হয় যা আমরা পূর্বেই উল্লেখ করেছি।

৪/ টার্গেটের ডিভাইস থেকে যোগাযোগ ট্র্যাকিং

যখন ভিক্টিমের ডিভাইসে ট্রোজান হর্স নামক ক্ষতিকারক সফটওয়্যার ঢুকানো হবে তখন তার পক্ষে সম্ভব অপারেটিং সিস্টেম ও যোগাযোগ সফটওয়ারের মধ্য দিয়ে অতিক্রম করা ভয়েস কল ট্র্যাক করা অথবা সরাসরি মাইক্রোফোন থেকেও আওয়াজ লুফে নেয়া এবং সে এগুলো গোপন ট্রোজান হর্সের মাধ্যমে ডাটা সংরক্ষিত করে রাখে। এবং এগুলকে উপযুক্ত যোগাযোগ নেটওয়ার্কের মাধ্যমে প্রেরণ করার জন্য উপযুক্ত সুযোগের অপেক্ষায় থাকে, তা হয়ত ইন্টারনেট ব্রাউজ করার সময় অথবা ওয়াইফাই এর মাধ্যমে এমনকি ব্লুটুথের মধ্য দিয়েও।

এখনি প্রশ্ন দেখা দিবে: যখন বিষয়টা এরকম হয়ে গেল,তখন নিরাপদ সিস্টেম কী? এবং কীভাবে আমাদের জন্য সম্ভব হবে যোগাযোগ সিস্টেমের উপর নির্ভর করা যেহেতু সকল সিস্টেম হ্যাক হওয়ার উপযুক্ত?

নিরাপদ সিস্টেম

আমরা এখন যোগাযোগের ক্ষেত্রে ব্যবহারকারীদের জন্যে সস্তা ডিভাইসের প্রয়োজনীয়তা ও টেকনোলজি ও নিরাপত্তার জন্যে কঠিন সিস্টেমের পরিবর্তে সহজে ব্যবহারযোগ্য সফটওয়ারের যুগে বাস করছি। তাই বলতে পারি যে, পূর্ন নিরাপদ যোগাযোগ সিস্টেম শুধু স্বপ্ন। তেমনিভাবে সেলুলার যোগাযোগ কোম্পানিও অতিরিক্ত প্রযুক্তিগত নিরাপত্তা, বিশেষ যোগাযোগ ডিভাইস ও জটিল সফটওয়্যার ব্যবহার করে গ্রাহকদেরকে হারাতে চায় না। এটা ঠিক যে, এই সমাধানগুলি পাবলিক যোগাযোগ কোম্পানিগুলির জন্য উচিতও না। কিন্তু এগুলো উপকারী ও গ্রহণযোগ্য হবে ব্যবহারকারীদের বিশেষ গ্রুপের জন্য, যাদের কাজের জন্য পূর্ণাঙ্গ ও বিশেষভাবে যোগাযোগের নিরাপদ পরিবেশ প্রয়োজন। তেমনিভাবে বিভিন্ন যেসব কোম্পানি ও প্রতিষ্ঠানের চাহিদা থাকে উঁচু পর্যায়ের সংরক্ষণ ও নিরাপত্তা।

ইমেইল সিকিউরিটি

" ফ্রিতে আজকাল কিছুই পাওয়া যায় না। যদি কোন জিনিস ফ্রিতে পাওয়া যায় তাহলে ভেবে নিন আপনিই তার পন্য।"

আমরা অধিকাংশ সময় ইমেইল গুগল ইয়াহু হটমেইল ও আইক্লাউডই ব্যবহার করি । একথা স্মরণ রাখবেন আপনি যে ইমেলই পাঠান বা ইমেলের মধ্যে যা কিছুই এটাচ থাকে এর সব কিছুই ঐ ইমেইলের কম্পানীর মালিকানা হয়ে যায়। চাই সে তা বিজ্ঞাপন দাতাদের কাছে বিক্রি করুক বা সরকারের কাছে বিক্রি করুক। কেননা সে যখন আপনাকে ফ্রিতে সার্ভিস দিচ্ছে তখন এটা স্পষ্ট যে আপনি এবং আপনার ডেটাই তার পণ্য। ফ্রিতে কোন কম্পানিই আপনাকে সার্ভিস দিবেনা। আর চারটি ইমেইল প্রাউডিটরের কথা আমরা পিছনে আলোচনা করেছি, এডওয়ার্ড স্নোডেন এই কোম্পানিগুলো কে প্রিজম প্রোগামের অংশ বলেছেন যে, এগুলো আমেরিকার গোয়েন্দা সংস্থাগুলোর জন্য তথ্য একত্র করে।

এর থেকেও বেশি সরলতা হলো আমরা আইক্লাউড ও গুগলে আমাদের পার্সোনাল সকল ফটো ব্যাকআপ করি এর থেকে আরো একধাপ এগিয়ে আমরা হোয়াটসআপ চ্যাটের ব্যাকআপও এগুলোর উপর করি যা কিনা আন-ক্রিপডেট এবং ইমেল প্রোভাইডর পড়তে সক্ষম।

এই ইমেল সার্ভিসগুলো এত নিরাপদ নয়, ইয়াহুর প্রায় অর্ধেকেরও বেশি আইডি হ্যাক হয়েছে। এছাড়াও এগুলোর ইনক্রাপশন বিশেষ কিছু নয়। এজন্য এগুলো কোনমতেই ব্যবহার করা উচিত নয়। তবে যদি কেহ নিজের পার্সোনাল আইডি আলাদা ল্যাপটপ বা মোবাইলে ব্যবহার করে আর তাতে কোন সন্দহজনক জিনিষ না থাকে তাহলে সুযোগ রয়েছে।

শুধু সেই ইমেইল ব্যবহার করুন যার ইনক্রিপশন বেশ ভালো থাকেঃ

1. protonmail
2. Tutanota
3. Mailfence

এর বিশেষত্ব এটাও যে proton ছাড়া বাকি দুটো এড্রেস করতে ফোন নাম্বারও চায় না । অধিকাংশ ব্যক্তি এরপর এই প্রশ্নটা করে যে আপনি বলেছেন ফ্রিতে কোন কেহ সার্ভিস দেয় না তো এরা কেন দিচ্ছে ??

প্রথম কথা হলো এরা ফ্রিতে শুধুমাত্র নির্দিষ্ট সংখায় কিছু ফিচার দেয়। যাতে আমরা অন্যান্য ফিচার ব্যবহারের জন্য তাকে ক্রয় করি আর তাও ২৫০ বা ৫০০ এমবি ফ্রি দেয় বাকি গুলো টাকায় বিক্রী করে। এছাড়া মানুষ তাদেরকে ডোনেশন করে, আপনি ওদের ওয়েবসাইটে যান ওখানে আপনি ডোনেশন অপশন দেখতে পাবেন এতে ওদের পর্যাপ্ত অর্থের যোগান হয়ে যায়।

এছাড়াও আরো ইমেল ব্যবহার করেন যেগুলোতে ভেরিফেকেশনের জন্য নাম্বার চায় না। যেমন Yandex ইত্যাদি। এগুলো যোগাযোগের জন্য ব্যবহার করা নিরাপদ নয়। যদি কোথাও একাউন্ট ভেরিফেকেশন করাতে হয় সেখানে Yandex এর ব্যবহার ঠিক আছে কিন্ত ইয়ানাডেক্স রুশদের কম্পানি। আর গুগল যেভাবে আমিরিকার জন্য কাজ করে, এই কম্পানির এমন নজির মিলেছে যাতে বুঝা যায় এই কম্পানি রুশদের জন্য গোয়েন্দাগিরি করে।

অনেকেই ভিবিন্ন জায়গায় একাউন্ট তৈরির জন্য ফেইক মেইল বা অস্থায়ী মেইল ব্যবহার করেন। যেমন ফেসবুকের এর একাউন্ট খোলার জন্য, সেখানে নিচেরগুলো ব্যবহার করতে পারেন।

https://emailfake.com/
https://generator.email/
https://temp-mail.org/en/

এগুলোতে গিয়ে একটা অস্থায়ী আইডি বানিয়ে ফেসবুকে ব্যবহার করুন। একথা স্মরণ রাখুন এই ধরণের ইমেল দ্বারা তৈরী একাউন্ট খুব সহজেই হ্যাক হতে পারে এজন্য এই ধরণের অস্থায়ী ইমেল দিয়ে কোন বিশেষ একাউন্ট তৈরী করবেন না। হ্যা যেখানে আপনাকে কোন অস্থায়ি একাউন্ট বানানোর প্রয়োজন সেখানে আপনি এমনটা করতে পারেন।

ক্লাউড স্টোরেজে তথ্য সংরক্ষণ

উত্তম ক্লাউড স্টোরেজ নির্বাচনঃ সাধারণ ক্লাউড স্টোরেজ যেখানে আমরা নিজেদের তথ্য সংরক্ষন করে থাকি অথবা অন্যদের জন্য কোন জিনিস আপলোড করি সেটা নিরাপদ থাকে না। বিশেষ ভাবে ড্রপবক্স ,আই ক্লাউড এবং গুগল ড্রাইভ। এরা গোয়েন্দা সংস্থাদেরকে আপনার তথ্য সরবরাহ করতে সক্ষম এবং প্রয়োজনে করে থাকে। বিশেষ করে প্রিজম প্রোগামে যত কম্পানি কাজ করে তাদের থেকে বেচে থাকা অত্যন্ত জরুরী। ক্লাউড স্টোরের ক্ষেত্রে আপনি অবশ্যই এটা লক্ষ রাখবেন, আপনার ডেটা সার্ভার, ইন্টারনেট, শেয়ারিং সব জায়গাতে এন্ড টু এন্ড ইনক্রিপটেড হয়।

সবচেয়ে উত্তম ক্লাউড স্টোরেজ যেখানে এই ফিচার বিদ্যমান সেগুলো হলো এইঃ

1. https://tresorit.com
সবচেয়ে ভালো এবং আপনার তথ্য পরিপূর্ণ ভাবে এন্ড টু এন্ড ইনক্রিপটেড রাখে তবে এটা পেইড স্টোরেজ।

2. https://teamdrive.com
এটাও খুব ভালো সার্ভিস দেয় কিন্তু এটাতেও টাকা দিতে হয়।।

3. https://Sync.com

সবচেয়ে উপযোগী সার্ভিস আর কম মূল্য রাখে। আর এতে আপনি ফ্রিতেও একাউন্ট তৈরি করত পারবেন যাতে ৫ জিবি পর্যন্ত ডেটা আপলোড করতে পারবেন।

আরো একটি ফ্রি বিকল্প রয়েছে যদি আপনি পয়সা খরচ করতে না চান। প্রথমে cryptomator ইনস্টল করে নিন। এটা ড্রপবক্স, গুগল ড্রাইভ ইত্যাদি সাধারণ ক্লাউড সার্ভিসের সাথে লিংক হয়ে আপনার ডেটাকে ইনক্রিপ্ট করে তাতে পাঠিয়ে দেয়। এতে করে গুগল আপনার তথ্য দেখতে চাইলেও দেখতে পারে না যে আসলে তথ্যটা কী? কারণ সেটা cryptomator এর মাধ্যমে ইনক্রেপটেড হয়। এজন্য গুগল ড্রাইভের সাথে অবশ্যই এটা ব্যবহার করুন।

https://cryptomator.org/

এখান থেকে ডাউনলোড করতে পারবেন। এটার এন্ড্রোয়েড ভার্সন আছে কিন্তু বেশ দামি, এজন্য আপনি উইনডোজ ভার্সন ব্যবহার করুন।

উন্মুক্ত সাইটের APPS ডাউনলোডের নিরাপত্তা

অনেক সময় ওপেন গ্রুপ বা চ্যানেলে বিভিন্ন apps সংক্রান্ত তথ্য ও আলোচনা প্রচার করা হয়। এসব apps এর নিরাপত্তা নিয়ে আলোচনা করাটা আমরা জরুরী মনে করছি।

FB অথবা TG গ্রুপগুলো প্রকাশ্য যোগাযোগ মাধ্যম। যেখানে সকল শ্রেণির লোকই বিদ্যমান থাকে। যদিও অধিকাংশ এডমিন ভাইয়েরা সর্বাধিক সতর্কতা অবলম্বন করতে চেষ্টা করে। কিন্তু গ্রুপেন অন্যান্য সদস্যগণ সতর্কতা অবলম্বনে অনেক ক্ষেত্রে ভুল করে ফেলে এবং গ্রুপে যেকোনো ব্যক্তির প্রচার করা যেকোনো apps ডাউনলোড করে ইনস্টল করতে থাকে। কিন্তু আমাদের এসকল apps ইনস্টল করা ও ডাউনলোড করার ক্ষেত্রে অবশ্যই সতর্কতা অবলম্বন করা উচিত।

আমাদের এই কথাগুলো বলার উদ্দেশ্য শুধুমাত্র অনলাইনে সতর্কতা অবলম্বন। আমাদের উদ্দেশ্য এই নয় যে, যারাই এসকল apps প্রচার করবে, তাদের সকলকে গুপ্তচর ভাবা হবে। কেননা এখানে অনেক আন্তরিক ব্যক্তিও কাজ করেন। কিন্তু খিজিরের বেশে কখনো ডাকাত

ঘুরে। অর্থাৎ গোয়েন্দাসংস্থা ম্যালাওয়ার বা বিভিন্ন হ্যাকিং সেটিং দিয়ে তৈরি apps ওপেন জায়গায় প্রচার করে থাকে। ফলে যে ব্যক্তি এগুলো ইনস্টল করে তার সকল ব্যক্তিগত ইনফরমেশন এবং মোবাইলের যাবতীয় গোপন তথ্য তাদের নজরদারীতে চলে যায়।

এর জন্যে মোবাইলের apps গুলো সবসময় F Droid, playstore এর নিরাপদ ভার্সন Yalpstore থেকে ডাউনলোড করবেন। এই সাইটগুলো ব্যতিত অন্য কোন সাইট থেকে apps ডাউনলোড করবেন না। কেননা ঐগুলোর সাথে গোয়েন্দা সংস্থাগুলোর সফটওয়্যার মিশে থাকার ভয় থাকে। যার ফলে তাদের সফটওয়্যারগুলো আপনার অজান্তেই নিজে নিজে আপনার মোবাইলে ইনস্টল হবে। যার দ্বারা আপনার সকল পরিচয় ও তথ্য লিক হয়ে যেতে পারে। এই জন্য যেকোনো গ্রুপে বা চ্যানেলে শেয়ার করা যেকোনো apps ইনস্টল করবেন না।

যখন কোনো apps ফ্রি তে না পাওয়া যাবে অর্থাৎ টাকা দিয়ে কিনে নিতে হয়, সেই ক্ষেত্রে তার crack version টি নির্ভরযোগ্য স্থান থেকে ডাউনলোড করবেন। সবসময় মোবাইলের apps গুলো update করবেন। আর যদি কোনো apps ওপেন কোনো গ্রুপ থেকে ডাউনলোড করতে চান তাহলে নির্ভরশীল কোনো চ্যানেল বা গ্রুপ থেকে ডাউনলোড করুন। অথবা নির্ভরশীল চ্যানেলে থেকে অন্য কোনো চ্যানেলের লিংক দেয়া থাকলে সেখান থেকে ডাউনলোড করবেন এবং এই বিষয়টিকে পুরোপুরি নিশ্চিত করে নিবেন যে, শেয়ার হওয়া অ্যাপটি নির্ভরশীল কোনো চ্যানেল থেকে শেয়ার হয়েছে।

Yalp store এপ ডাউনলোড

নিরাপদ সফটওয়্যার নামানোর মাধ্যম yalp store ব্যবহার করুন। যেটা পূর্ণভাবে গুগল প্লে স্টোর এর পরিবর্তিত মাধ্যম। সেখানে কোনো gmail id প্রয়োজন হয়না এবং সেটা 1 mb এর কম। আপনার পূর্ন নিরাপত্তা রক্ষা করবে ও ওপেন সোর্স যা ফ্রিতে পাওয়া যায়।

প্রথমে নিচের লিঙ্ক থেকে f-droid ডাউনলোড করে নিন।

https://f-droid.org/FDroid.apk

install দেওয়ার পর software এ যান। software এ ক্লিক করুন তারপর সমস্ত app update হওয়ার জন্য কিছুক্ষণ অপেক্ষা করুন। অতঃপর সার্চ বাটনে ক্লিক করুন এবং yalp লেখুন তখন আপনার সামনে yalp store চলে আসবে। সেখান থেকে ইন্সটল দিন।

install দেওয়ার পরে সেটি চালু করুন। প্রথমে আপনার কাছে দুইটি অপশন আসবে, একটি হচ্ছে google id দিয়ে অন্যটি হচ্ছে ফেক আইডি দিয়ে সফটওয়্যার নামানো জন্য। আপনি ফেক আইডিতে ক্লিক করুন ও উপরের সার্চ বাটনটা ব্যবহার করুন এবং আপনার যা ইচ্ছা ডাউনলোড করুন। সেখান থেকে আপনাকে সেই ফলাফল প্রকাশ করবে যা গুগল প্লে-ষ্টোরে প্রকাশ করা হয় এবং সাথে সাথে এখান থেকে update এর কাজ করতে পারবেন।

তা আপনাকে পূর্ণভাবে গুগল প্লে স্টোর থেকে মুক্তি দিবে এবং অন্যান্য চ্যানেল থেকেও গুগল প্লে স্টোরের লিংকগুলো এর মাধ্যমে ওপেন করতে পারবেন।

EDS - মোবাইলে ফাইল গোপন করুন

EDS (Encrypted Data Store) হচ্ছে এন্ড্রয়েডের ফাইল গোপনের সফটওয়্যার, যা ফাইল সমূহকে গোপনীয় কন্টেইনারের মধ্যে লুকাবে। যেমন আমরা পিসিতে VeraCrypt বা TrueCrypt এর মাধ্যমে করে থাকি। এবং এটা দিয়ে VeraCrypt(R), TrueCrypt(R), LUKS, EncFs, CyberSafe(R ইত্যাদি দিয়ে বানানো ফাইলগুলো সাপোর্ট করে। অর্থাৎ এতা দিয়ে বানানো ফাইল পিসিতে নিয়ে VeraCrypt দিয়ে খুলতে পারবেন এবং পিসিতে বানানো ফাইলও মেমুরীর মাধ্যমে এটা দিয়ে মোবাইলেই খুলতে পারবেন। এই প্রোগ্রাম দুইভাবে কাজ করেঃ non-mounted এবং mounted.

EDS দুই ভার্সন পাওয়া যায়। এটা হচ্ছে পেইড ভার্সন। অন্যটা হচ্ছে "lite" ভার্সন যা ওপেন সোর্স। অর্থাৎ এটাকে অন্যান্য ওপেন সোর্স এপ্লিকেশনের মত নিজের মত পরিবর্তন বা পরিবর্ধন করতে পারবেন।

এই Program এর সমস্ত features সমূহ দেখতে নিচের লিংকে প্রবেশ করুনঃ
https://sovworks.com/eds/index.php

EDS ব্যবহারের পদ্ধতিঃ (বাংলায় ছবির মাধ্যমে)

অনলাইনে পড়ুন

https://pastethis.at/xW1pfFVuY06j1

PDF ডাউনলোড

https://archive.org/download/fulergran_protonmail_EDS/EDS%20.pdf

কিভাবে VeraCrypt কন্টেইনার বানাবেন ও খুলবেন এবং সাধারণ গোপনীয় flash card বা container বানাবেন ও খুলবেন তার ভিডিও টিউটেরিয়াল দেখতে নিচের লিংকে প্রবেশ করুন। এখানে প্রত্যেকটার আলাদা আলাদা টিউটেরিয়াল সুন্দর ভাবে দেয়া আছে। https://sovworks.com/eds/managing-containers.php

Mount container - যদি আপনার মোবাইল রুট করা থাকে তো ফাইলের জন্যে টেম্পরারী কোন ফাইল ব্যবহারের প্রয়োজন নেই বরং FAT ও NTFS ফাইলগুলোকে sd card এর মত গোপন ও খুলতে পারবেন। যার ভিতরে থাকা ফাইলগুলো খুলা অবস্থায় গ্যালারী ও ফাইল ম্যানেজারের মাধ্যমে চালাতে পারবেন। টিউটেরিয়ালঃ https://sovworks.com/eds/mounting-a-container.php

Dropbox বা Sync এর মত ক্লাউড স্টোরেজ এর ফাইলকেই পাসওয়ার্ড প্রটেক্ট করে গোপন করতে পারবেন। টিউটেরিয়ালঃ

https://sovworks.com/eds/cloud-storages-and-container-synchronization.php

ভিপিএন ব্যবহার

ভিপিএন ব্যবহারের উপকারিতা

১/ ইন্টারনেটে আপনার আইপি এড্রেস এবং লোকেশন প্রকাশ পায়না। ট্রাফিক ইনক্রেপ্টেড থাকবে, ইনক্রিপশনের কারনে আপনার সিকিউরিটি আরো জোরদার ও উত্তম হবে। ইন্টারনেটে যা করবে তা এজেন্সি, হ্যাকার, এবং আই.এস.পি এর দৃষ্টিতে আসবেনা।

৩/ ব্লক লিস্টে থাকা জিনিষ সমুহের বার্তা পর্যন্ত আদান প্রদান সম্ভব হয়ে যায়। যেমন: বর্তমানে পাকিস্থানে টেলিগ্রাম ব্লক লিস্টে আছে। তবে ভিপিএন এর মাধ্যমে ব্যবহার করতে পারে।

৪/ পাব্লিক ওয়াই ফাই ব্যবহার করার সময় হ্যকিং এর আশংকা থাকে কিন্ত আপনি পাব্লিক ওয়াই ফাই ভিপিএন এর সাহায্যে কোন ধরনের ভয় ভীতি ছাড়াই চালাতে পারবেন।

৫/ যেভাবে মন চায় সেভাবে ই আপনি ইন্টারনেট ব্যবহার করতে পারবে, কারো ভয় হবে না।

ভিপিএন অথবা গোয়েন্দা সফটওয়্যার

এন্ড্রয়েড ভিপিএন এর ব্যপারে একটা রিসার্চ হয়েছে। তার মধ্যে এন্ড্রয়েড ভিপিএন গুলোকে অসংখবার টেস্ট করা হয়েছে। ফলাফল এই যে, মোবাইল ভিপিএন এর ৭৫% আপনার উপর গোয়েন্দাগিরি করে। আর ৮২ % আপনার ডাটা পারমিশন চায়। এবং ৪০% মুবাইলে ম্যালাওয়ার, ভাইরাস এবং গোয়েন্দা সফটওয়্যার হিসেবে কাজ করে। তার মধ্যে প্রশিদ্ধ নাম করা ভিপিএন এর নাম রয়েছে যেগুলো ম্যালাওয়ার প্রমাণিত হয়েছে। যা লাখ নয় বরং কোটি বার ডাউনলোড হয়েছে।

তার মধ্যে Betternet VPN কোটি বার ডাউনলোড হয়েছে। টেস্টে গোয়েন্দা ম্যালাওয়ার যুক্ত দশ ভিপিএন এর মধ্যে তার নাম রয়েছে। এ ছাড়া ও প্রশিদ্ধ ভিপিএন এর মধ্যে Cyberghost, CM Data Manager, Easv VPN, VPN Master ইত্যাদি রয়েছে।

বিস্তারিত রিপোর্ট পড়ার জন্য আমরা ইংরেজি রিপোর্ট এবং তার লিংক এখানে শেয়ার করছি। যাদের পুরো সূচি এবং বিস্তারিত পড়ার প্রয়োজন তারা এখান থেকে পড়ে নিবে।

https://archive.org/download/paper-1/paper-1.pdf

এটা অধিকাংশ ফ্রি ভিপিএন এর মধ্যে পাওয়া যায়। কিন্তু আফসুসের বিষয় হল, টাকা দিয়ে ক্রয় করা কিছু ভিপিএনও গোয়েন্দাগিরি করে। এবং আমাদের ডাটা ও তথ্য সমুহের পারমিশন নিয়ে নেয়। অর্থাৎ আমরা টাকা দিব আবার গোয়েন্দাগিরির শিকার হব।

এই রিপোর্ট আপনাদের সামনে পেশ করার উদ্দেশ্য হল এন্ড্রয়েড ভিপিএন ব্যবহার করার ব্যাপারে সতর্কতা। এবং শুধু নির্ভরযোগ্য ভিপিএন ব্যবহার করা। আর বিশেষ ভাবে ফ্রি ভার্সন তো কোন ভাবেই ব্যবহার করবে না।

ভিপিএন নির্বাচন

১। ভিপিএন অবশ্যই ম্যলাওয়ার, ট্রেকার ও ব্রাউজার হ্যকিংয়ের মতো স্ক্রিপ্ট থেকে মুক্ত হতে হবে। এটা চেক করার জন্যে আপনি যখন কোন ভিপিএন ডাউনলোড করবেন তহন ব্যবহারের আগে এই অয়েব সাইটে এন্ড্রয়েড আইপি ফাইলটি চেক করুন।

https://www.virustotal.com/#/home/upload

যদি এক বা একাধিক এন্টি-ভাইরাসে আক্রান্ত দেখায় তাহলে অবশ্যই ব্যবহার করবেন না। এছাড়াও দেখবেন যাতে তারা আপনার মোবাইল ডিভাইস থেকে কোন ডাটা পারমিশন না চায়। যাদি চায় তো ব্যবহার করা যাবেনা।
এখানে উইন্ডোজ সেটাপের কথা বলা হয়নি কারন সেখানে জাসুসী কমই করা যায়। কাজেই এন্ড্রয়েডের ক্ষেত্রে বেশি সচেতন থাকতে হবে।

২। ভিপিএন কোন লগ'স না রাখতে হবে। লগ'স কয়েক ধরনের হয়ে থাকে।

ব্যবহারিক অথবা ব্রাউজিং লগ'সঃ এই লগ'স আপনার সমস্ত আইপি এড্রেস, তথ্য এবং হিস্ট্রি নিজের কাছে সংরক্ষন করে। যদি কোন ভিপিএন এমন লগ'স রাখার সিস্টেম থাকে তাহলে কোন ভাবেই ব্যবহার করা যাবেনা।
কানেকশন লগ'সঃ এই লগ'স আপনার নেট ব্যবহারের যাবতীয় তথ্য নিজের কাছে রাখে। যেমন আপনি কখন কোথায় নেট ব্যবহার করেছেন সেটা সংরক্ষন করে। পরবর্তীতে কোম্পানী

এসব তথ্য প্রতিদিন বা কিছু দিন পরে ডিলেট করে দেয়। এটা তারা করে নিজেদের ভিপিএন নেটয়ার্ককে আরো শক্তিশালী করার জন্যে।

৩। তাদের ইনক্রিপশন এবং ইনক্রিপশন প্রটোকলকে অবশ্যই দেখতে হবে।

৪। এটাও দেখতে হবে যে এতে যেন আইপি এড্রেস প্রকাশিত হওয়ার আশংকা আছে কিনা। যেমনঃ Ivp6, Webrtc, DNC leaks এগুলোর মাধ্যমে সাধারনত ভিপিএনের আইপি প্রকাশিত হয়ে থাকে। কাজেই এমন ভিপি এন ব্যবহার করতে হবে যা এগুলোকে নষ্ট করে দিবে।

৫। এটাও দেখতে হবে যে এই ভিপি এন এই পাঁচ দেশের কোন একদেশের কোম্পানির তৈরী কিনা। পাঁচ দেশ হলো: USA, Canada, Australia, Uk, Barbados

৬/ ফ্রী ভিপিএন তো কোন অবস্থাতেই ব্যবহার করা যাবে না।

ভাল VPN লিস্ট

যেহেতু এই সমস্ত বিষয় সব ভিপিএনে দেখা কঠিন তাই এখানে একটা তালিকা দিচ্ছি এর মধ্য থেকে যেকোন একটা ব্যবহার করা যেতে পারে। এখানে তারতীব অনুযায়ী দেওয়া হলো অর্থাৎ নিচেরটা থেকে উপরেরটা ভাল।

1. VPN.AC
2. VPN Area
3. Nord VPN
4. Parfect Praivacy
5. Typr VPN

এই পাঁচটা ভিপিএন কোন লগ'স রাখে না এবং সকল প্রকার লিক ধংস করে দেয়। যদি আপনি ব্রাউজার থেকে Webrtc বন্ধ নাও করেন তবুও এই ভিপিএন ব্যবহারের ফলে Webrtc এর মাধ্যমে আপনার আইপি প্রকাশিত হবেনা।

তাছাড়া Express VPN স্পিড এবং অন্যান্য বৈশিষ্টের কারনে ১ নাম্বারে আছে। কিন্তু এর মধ্যে বড় ধরনের একটি সমস্যা হলো এটি বৃটিশ ভার্জিন আইলেন্ডের। আরেকটা ঝামেলা হলো এর মধ্যে কিছু কানেকশন লগ'স আছে। তবে নিরাপত্তা বিশেষজ্ঞরা এটাকেও ব্যবহার করার পরামর্শ দেন। তবে উপরের ৫ টা প্রাধান্য দেন। তাই আপনিও এটা ব্যবহার করতে পারেন তবে উপরের গুলোই প্রাধান্য পাবে।

নোটঃ এই ভিপিএনগুলোকে আপনি বিটকয়েনের মাধ্যমে সহজেই কিনতে পারেন এবং এতে আপনার কোন প্রকার তথ্য যেমন নাম পরিচয় ইত্যাদি কিছুই ফাস হবেনা।

F-Secure Freedome VPN এফ সিকিউর ফ্রিডমঃ এই ভিপিএন কানেকশন লাগেজ রাখে। কোন কোন বিশেষজ্ঞের মতে এটা নেট ব্যবহারের যাবতীয় লগ'স সংরক্ষন করে। এজন্য এটাকে এই তালিকায় আনা হয়নি। তবে এটা সিকিউরিটি এবং ইনক্রিপশনের ইত্যাদির দিক থেকে ভালো। যদি আপনি এটাকে মোবাইল রোট করার মাধ্যমে ফ্রি ব্যবহার করতে পারেন তাহলে করতে পারেন। তবে কেনার পরামর্শ আমরা দেইনা।

বিশ্বের সমস্ত ভিপিএনের পূর্ন বিশিষ্টগুলো একটি এক্সেল ফাইলের মধ্যে একত্রিত করা হয়েছে। যদি আপনার ভিপিএন যাচাই করতে চান অথবা তুলনা করতে চান তাহলে এখানে দেখে নিন। প্রাইভেসীর ৩ টা জায়গা যদি সবুজ হয় তাহলে সেটা ব্যবহারের অনুমতি মিলবে।

https://archive.org/download/VPNComparisonChart/VPN%20Comparison%20Chart.xlsx

Vpn kill switch

ভিপিএনের প্রয়োজনীয়তা নিয়ে পূর্বে অনেক আলোচনা হয়েছে, সামনেও হবে। এটা অচিরেই আবশ্যকীয় হয়ে পরবে। এখন হয়ত ভিপিএন ছাড়াও বাচা যাচ্ছে। কিন্তু এক সময় হয়ত ভিপিএন ব্যবহার না করা ফলে ড্রোনের টার্গেটে পরিনত হবে।

ভিপিএন ব্যবহারের ক্ষেত্রে সবচেয়ে ভয়ের বিষয় হল, মাঝে মাঝে VPN কানেকশন বন্ধ হয়ে যায়। তখন সবকিছু মূল IP দিয়েই চলতে থাকে। আর তা আপনার ISP (Internet service provider) জানতে পারে এবং স্টোর করে রাখে। ফলে যে কেহ সেখান থেকে আপনার তথ্য

সংগ্রহ করে নিতে পারে।

তাই আপনাকে সর্বদা VPN kill switch ব্যবহার করতে হবে। এটার কাজ হবে ভিপিএন কানেকশন বন্ধ হয়ে যাওয়া মাত্রই আপনার সমস্ত নেট সার্ভিস বন্ধ করে দেয়া। যার ফলে আপনার নিরাপত্তা বজায় থাকবে। এটা পিসি ও এন্ড্রয়েড সমস্ত ডিভাইসেই ব্যবহার আবশ্যক।

প্রথমত এন্ড্রয়েডে কিছু VPN এপ kill switch সুবিধা দিয়ে থাকে। কিন্তু সবগুলোর ব্যবহার নিরাপদ নয়, যা আমরা পূর্বের পোষ্টে বলেছি। যেগুলো এই সুবিধা দেয়া তার মধ্যে আছে PIA vpn, Vyprvpn, pure vpn, Xpress Vpn, Nord Vpn. তবে এখানে সবগুলো ব্যবহারের উপদেশ দিব না। কারণ PIA vpn হচ্ছে usa তৈরি, VyprVpn আপনার সমস্ত connection logs সংরক্ষন করে, pure vpn যে হ্যাকাররা লিক করে ফেলেছে তা তো প্রশিদ্ধ। কিছুদিন আগে USA তে Ryan Lin নামের এক সাইবার অপরাধীকে pure ব্যবহার সত্যেও গ্রেফতার করা হয়েছে।

Xpress vpn হচ্ছে British Virgin Islands-based company পরিচালিত। তবে নিরাপত্তা বিশেষজ্ঞরা এটা ব্যবহারে অনুমতি দিয়ে থাকেন। কিন্তু এটা মাত্র ৩ মাস ফ্রী ব্যবহার করা যায়।

সবচেয়ে ভাল হচ্ছে Nord Vpn যা টর এর পরেই সবচেয়ে নিরাপদ মাধ্যম। তারাও kill switch এর সুবিধা দিয়ে থাকে। তাদের ওয়েব সাইটে দেখুন:

https://nordvpn.com/features/kill-switch-technique/

এখানে vpn চালু করে setting থেকে Always-ON ফিচারটি চালু করে দিতে হবে। এটা আগে ফ্রীতে ব্যবহার করা গেলেও ইদানীং ফ্রীতে ব্যবহার করা অসম্ভব হয়ে পরেছে।

আলাদা ভাবেও kill switch ব্যবহার করা যায়। তবে তার জন্য গুরুত্বপূর্ণ হচ্ছে সেই app টা ওপেন সোর্স হতে হবে, অন্যথায় ব্যবহার করা নিরাপদ নয়। নিচের লিংকে একটা Opensource kill switch দেয়া হল।

https://www.privateinternetaccess.com/forum/discussion/18036/tutorial-better-killswitch-and-ipv6-leak-protection-on-android-with-afwall-requires-root

এটার জন্য মোবাইল রুট করতে হবে। আফসোসের বিষয় হল linux, windows or mac এর জন্যে ইন্টারনেটে যেমন ভাল kill switch সচরাচর অনেক পাওয়া যায়, Android এর জন্য তেমন পাওয়া যায় না অথবা সাচ্ছন্দে ব্যবহার করা যায় না।

টরের VPN ও proxy ব্যবহারে সতর্কতা

আমরা অনেক সময় টরের মাধ্যমে অন্যান্য App/software চালাই কিংবা টর proxy সকস ইউজ করে থাকি। যাতে করে সেই সফটওয়্যারগুলো টরের মাধ্যমে পরিচালিত হয়। যেমন ভিবিন্ন ব্রাউজার, টেলেগ্রাম বা অন্য কিছু। কিন্তু এই ক্ষেত্রে অনেক সময় DNS leak হয়ে আপনার IP প্রকাশিত হয়ে পরে। কারণ সমস্ত ভিপিএনের নিজস্ব DNS server থাকে যা দিয়ে তারা কোন ওয়েবে ঢুকার সময় dns resolve করে কিন্তু টরে সে জিনিসটা তেমন ভাবে করে না, ফলে ১ সেকেন্ডের জন্যে আপনার নিজস্ব DNS ব্যবহার হলে আপনার ISP (Internet service provider) জানতে পারবে আপনি কোন কোন সাইট এর জন্য domain resolve করেছেন। এই ব্যপারে সয়ং টরের অফিসিয়াল সাইটেই আর্টিকেল আছে। সেখানে সাধারণ ভাবে অন্যান্য ব্রাউজার বা সফটওয়্যারকে টর দিয়ে ব্যবহার বিপদজনক বলা হয়েছে। এই লিংকে দেখুনঃ

https://www.torproject.org/docs/faq.html.en#CompatibleApplications
ওই লিংক থাকা এই সংক্রান্ত কথা নিচে দেয়া হল:

"What programs can I use with Tor?
Most people use Tor Browser, which includes everything you need to browse the web safely using Tor. Using other browsers is dangerous and not recommended.
There are plenty of other programs you can use with Tor, but we haven't researched the application-level anonymity issues on all of them well enough to be able to recommend a safe configuration. Our wiki has a community-maintained list of instructions for Torifying specific applications. Please add to these lists and help us keep them accurate"

তবে এটা সব application/software এর ক্ষেত্রে ঘটে না। এজন্য কোন software কে tor দিয়ে চালানোর আগে টেস্ট করতে হবে আসলেই কি এই software টি DNS leak করে কি না। এটার জন্য এক ধরনেরর টুল আছে যার নাম wireshark. এই সফটয়ারের dns leak যে হবে সেটার প্রমান আপনি wireshark দিয়ে পাবেন। wireshark একটা জনপ্রিয় টুল যেটা দিয়ে কোন নেটওয়ার্ক এর আন্ডারে যত ইউজার থাকে সবার উপর নজর রাখা যায়।

https://en.m.wikipedia.org/wiki/Wireshark

Wireshark এর অফিসিয়াল সাইট থেকে সফটওয়্যার ডাউনলোড করতে পারবেন এবং সেখানেই user গাইডসহ বিস্তারিত সব কিছুই পাবেন।

https://www.wireshark.org/download.html

তাই শিউর হয়ে নিন কোন অ্যাপ টর দিয়ে চালানো উচিত নয়। Orfox এপ চালানোতে কোন সমস্যা নেই।

টরের নিরাপত্তা ভঙ্গকারী - Correlation Attack

সারা বছর ধরে অনেক টর ব্যবহারকারী তাদের গোপনীয়তা হারিয়েছে। এখানে "Correlation Attack" নামে একটি কৌশল ব্যাখ্যা করতে যাচ্ছি যা সরকারি সংস্থা ব্যবহার করে থাকে।

টর ব্যাপক ব্যবহার শুরু হওয়ার পর এই আক্রমণটি শুরু হয়েছে। এখানে আক্রমণকারী টর সার্কিটের প্রথম এবং শেষ রাউটার নিয়ন্ত্রণ করে সেগুলো পর্যবেক্ষণ করে এবং পারস্পরিক সম্পর্কযুক্ত তথ্য ও টাইমিং এর মাধ্যমে টরের গোপনীয়তা লঙ্ঘন করে।

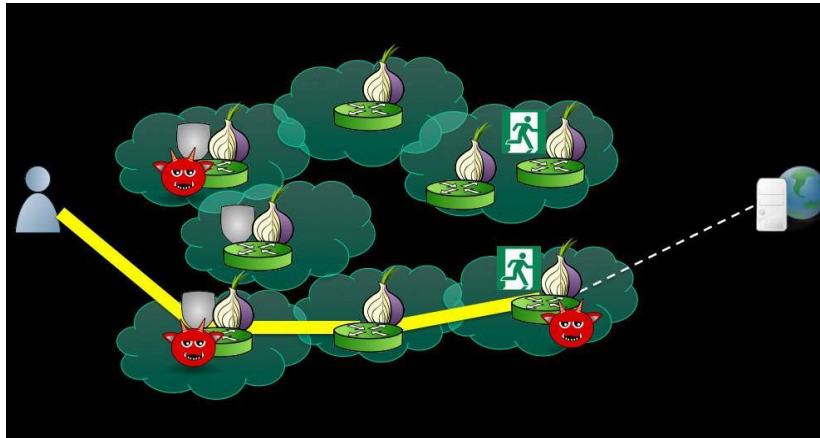
এই আক্রমন প্রতিরোধ করতে কোন প্যাচ তৈরি করা যায় না, কারণ এটি কোনও বাগকে নয়। বরং গণিত (সম্ভাব্যতা এবং পরিসংখ্যান) ব্যবহার করে এবং টর নেটওয়ার্ক এর পদ্ধতি ব্যবহার করেই আক্রমণ করা হয়।

আক্রমণ সফ্টওয়্যারকে লক্ষ করে নয় বরং ব্যবহারকারীদের বিরুদ্ধে করা হয়। উদাহরণস্বরূপ, যদি অপরাধী টর ব্যবহারকারী নিজের state, বয়স অথবা অতীতের অপরাধমূলক কার্যকলাপগুলি সম্পর্কে কোন তথ্য শেয়ার করে, তবে সরকারী সংস্থা সেই এলাকার সমস্ত সম্ভাব্য সন্দেহভাজনদের ইন্টারনেট কার্যকলাপ নিরীক্ষণের করে এবং দেখে যে কোন টর নেটওয়ার্কে এই

ব্যক্তি একই সময়ে অনলাইন আসে।

একটু বিশদ বিশ্লেষণ করি, টরের মধ্যে তিনটা রিলে ব্যবহার করা হয়, প্রথমটা আপনার IP যা আপনার IPS এর জানা থাকে। দ্বিতিয়টা টরের রিলে ও তৃতীয়টা যে অয়েব সার্ভারে প্রবেশ করেছেন সেটার এক্সিট রিলে। এখন তারা সারা দেশ থেকে সন্দেহজনক সমস্ত আইপি টার্গেট করবে এবং নির্দিষ্ট অয়েব সার্ভারের সমস্ত exit relays পর্যবেক্ষন করবে। পরে সেই সাইটের ব্যবহারকারী ও টার্গেটেড আইপিগুলোর অনলাইনে আসার সময় মিলিয়ে তারা ফাইনাল করে যে তারাই এই সময়গুলোতে সেই সাইটে ঢুকেছিল।

এটা ইতিমধ্যে স্পষ্ট যে এই আক্রমণটি ভাল পৃষ্ঠপোষকতা প্রয়োজন এবং বেশিরভাগ সরকারি সংস্থার দ্বারা পরিচালিত হয়। এই পিছনে কারণ টর 7000 রিলে এবং বেশী 2 মিলিয়ন দৈনিক ব্যবহারকারীর সংখ্যা।

যেহেতু টর স্বেচ্ছাসেবক ব্যবহার করে, তাই টর নেটওয়ার্ককে সাহায্য করার জন্য আপনি যত ইচ্ছা relay দিতে পারবেন। এবং টর কম্পানী আপনার সার্ভারকে তাদের কাজে ব্যবহার করবে। টরের রিলেগুলির একটি বিশাল অংশ যেহেতু সেচ্ছাসেবকদের থেকেই আসে তাই তারা নিজেদের রিলেগুলো নিয়ন্ত্রণ করে এবং কোন সেচ্ছাসেবকের জন্য একই ব্যবহারকারীকে গার্ড এবং এক্সিট রিলে পরিবেশনের সুযোগ থাকে। ফলে এটা শুধুমাত্র টাইমিং এর ব্যাপার যে আপনি কখন সার্কিট ব্যবহার শুরু করেছেন।

কার্নেগী মেলন ইউনিভার্সিটি থেকে টর্ নেটওয়ার্কে সর্বপ্রথম correlation attack করা হয়। এবং FBI এর কাছে টর ব্যবহারকারীদের তথ্য 1 মিলিয়ন মার্কিন ডলারে বিক্রি করা হয়েছিল। এটার হয়েছিল 2014 সালে। এই আক্রমণটি হয়েছি যে সমস্ত ওয়েবসাইট Silk Road 2.0

ব্যবহার করে এবং ২টা child porn সাইট।

ভাল খবর হচ্ছে টর ব্যবহারকারীদের এই আক্রমণ সম্পর্কে সচেতন করছে। এবং টর প্রকল্পটি ইতোমধ্যে প্রযুক্তিগুলির উপর কাজ করছে যাতে ওয়েবসাইটের ফিঙ্গারপ্রিন্টিং হামলাগুলি কম কার্যকর করে।

এটার সমাধান হিসেবে টর নেটওয়ার্কে সংযোগ হওয়ার জন্য একটি বিশ্বস্ত ভিপিএন ব্যবহার করা আবশ্যক কারণ তাতে correlation attack আপনার IP প্রদান করবে না। তবে আক্রমণকারী আপনার টরের প্রক্সি সার্ভারের একজন। তাই কখনো কোন গ্রুরুত্বপূর্ন মেসেজ ইনক্রীপ্ট করা ছাড়া প্রেরন করবেন না।

যেহেতু সমস্ত ভিপিএন logs রাখে ও টাকা দিতে তা সরকারের কাছে বিক্রি করার ভয় থাকে এবং অন্য দিকে টরের মধ্যেও আইপি প্রকাশের আশংকা থাকে তাই "VPN + Tor sucks" পূর্ন নিরাপত্তা নিশ্চিত করবে। একটাতে সমস্যা হলে অন্যটা তা প্রতিরোধ করবে ইনশাআল্লাহ।

Tor Messenger ঝুকিপূর্ন

টর মেসেঞ্জার হচ্ছে এমন একটি মেসেজিং প্লাটফর্ম যার দ্বারা টর সার্ভারের মাধ্যমে নিরাপদ যোগাযোগ করা হয়। এতে OTR (Off-the-Record) এর মাধ্যম one-to-one কনভার্সেশন হয়ে থাকে অর্থাৎ একজনের ডিভাইসের সাথে আরেকজনের ডিভাইসের সরাসরি যোগাযোগ করিয়ে দেয়া হয়, মাঝে কোন সার্ভারে তথ্য জমা বা পরিবর্তন করা হয় না।

টর ব্রাউজার তৈরি করা হয়েছে জনপ্রিয় মেসেজিং ক্লায়েন্ট Instantbird এর উপর ভিত্তি করে। যার ফলে Instant মেসেজিং এর সমস্ত প্রটোকল দিয়ে এটাতে মেসেজিং করা যায়। যেমন Jabber (XMPP), IRC, Google Talk, Facebook, Twitter ইত্যাদি।

তবে সমস্যা হচ্ছে এই Instantbird টর কোম্পানির সার্ভিস নয়। বরং এটা Mozilla কমিউনিটির পক্ষ থেকে তৈরি করা। আর তারা এখন Instantbird কে ডেভলাপ করে না। কারণ তারা এটা বাদ দিয়ে Thunderbird নামে নতুন একটি মেসেজিং ক্লায়েন্ট তৈরি

করেছে। এর অর্থ হচ্ছে Instantbird এর মধ্যে যদি সমস্যা দেখা দেয় তা আর ঠিক করা হবে না। ফলে টর মেসেঞ্জারের সমস্ত ব্যবহারকারী অনিরাপদ হয়ে পড়বে। আর এটা নাকি হয়েও গেছে। অর্থাৎ মেটাডাটায় প্রোব্লেম হয়ে OTR support লিক হয়ে গেছে। কিন্তু এটা আর কখনোই সমাধান করা হবে না। ফলে টর মেসেঞ্জারের মূল নিরাপত্তা নষ্ট হয়ে মেসেজ মধ্যের কোন সার্ভারে জমা হওয়ার ঝুকি সৃষ্টি হয়ে গেছে। বিস্তারিত দেখুন টরের অফিসিয়াল সাইটেঃ

https://blog.torproject.org/sunsetting-tor-messenger

যার ফলে টর মেসেঞ্জারের অফিসিয়াল ডাউনলোড পেইজেই এটা ব্যবহার করার ক্ষেত্রে নিষেধ করে দেয়া হয়েছে। সেখানে বলা হয়েছে, As of March 2018, Tor Messenger is no longer maintained and you should NOT use it. ডাউনলোড পেইজে দেখুনঃ

https://blog.torproject.org/tor-messenger-beta-chat-over-tor-easily

তাই সমাধান হচ্ছে নিরাপত্তার খাতিরে টর মেসেঞ্জার একেবারেই ব্যবহার না করা, বরং Jabber এর মাধ্যমে মেসেজিং এর অন্যান্য সফটওয়্যার যেমন pidgin ইত্যাদি ব্যবহার করা। অথবা একান্তই যদি ব্যবহার করা হয় তাহলে মেসেজ অবশ্যই PGP এর মাধ্যমে গোপন করে পাঠাতে হবে।

BBM চালানোর পদ্ধতি

এন্ড্রয়েডে এমন অনেক সফটওয়্যার আছে যারা দাবী করে যে তারা End to End Encrypted মেসেজ পাঠায়। অর্থাৎ মেসেজকে কোডের মাধ্যমে পরিবর্তন করে আদান-প্রদান করে যার ফলে যে পাঠাচ্ছে এবং যার কাছে পাঠাচ্ছে , এই দুই ব্যক্তি ছাড়া অন্য কেহ জানবে না কি পাঠানো হচ্ছে। এমকি কেহ যদি নজরদারীও করে সেও জানতে পারবে না আপনি কি মেসেজ পাঠাচ্ছেন। কিন্তু অধিকাংশ সফটওয়্যারের ক্ষেত্রে এটা ভুল প্রমানিত হয়েছে। বিশেষ করে whatsapp এর মেসেজ অধিকাংশ হ্যকারই ট্র্যাক করতে সক্ষম হয়েছে। যার ফলে এগুলোর উপর ভরসা করা যায় না। কিন্তু BBM এর ক্ষেত্রে হ্যাকারদের পক্ষ থেকেই সত্যায়ন করা হয়েছে যে এটার মেসজ কোডিং করে পাঠানো হয়। যার ফলে তৃতীয় কেহ জানতে পারে না কি মেসেজ পাঠানো হয়েছে। তার পরেও সতর্কতাবসত প্রক্সি ব্যবহার করে মেসেজিং এর জন্যে ব্যবহার করা যায় ইনশাআল্লাহ।

ডাউনলোড লিংকঃ

http://www.1mobile.com/bbm-1125780.html

অথবা

https://play.google.com/store/apps/details?id=com.bbm

ডাউনলোড হওয়ার পর ইন্সটল করুন। এবং BBM এপকে ওপেন করুন।

১. শুরুতেই একাউন্ট খুলার অপশন আসবে। প্রথম বক্সে নাম দিন যা আপনি BBM এ ব্যবহার করতে চান। এমন নাম যা অন্য নামের সাথে না মিলে। দ্বিতীয় বক্সে ইমেইল দেন। তৃতীয় বক্সে পাসোয়ার্ড দিয়ে create ক্লিক করুন। এবং ইমেইল চেক করে দেখুন একটা লিংক আসবে সেটাতে ক্লিক করে একাউন্ট ভেরিফাই করুন।

২. যখন BBM এর মধ্যে সাইন ইন সম্পন্ন হবে find friends নামের একটা স্ক্রিন আসবে, সেখানে স্কিপ দেন।

৩. আপনার সামনে মূল স্ক্রিন ওপেন হবে, সেখানে উপরে বাম কোনায় তিন দাগের উপর ক্লিক করুন।

৪. সেখানে আপনার নামের উপর পিকচারের স্থানে ক্লিক করুন।

৫. এখানে এসে স্ক্রিনের মাঝের দিকে আপনি একটি পিন নাম্বার পাবেন যা অন্যদেরকে দিবেন আপনাকে ফ্রেন্ড বানানোর জন্য। এখান থেকে ব্যাক করেন।

৬. এখান আপনি আপনার ফ্রেন্ড মেনুতে যেন, সেখানে নিচে ডান দিকে ফ্রেন্ড যোগ করার অপশনে ক্লিক করুন।

৭. Add by PIN ক্লিক করুন ও আপনার বন্ধুর পিন নাম্বার দিন। তার কাছে ইনভাইটেশন যাবে, সে গ্রহন করার পর থেকে মেসেজিং করতে পারবেন।

BBM কে বন্ধ করার নিয়মঃ BBM এর মধ্যে একটা ঝামেলা হচ্ছে বের হয়ে আসার পরেও সর্বদা চলতে থাকে। যার জন্যে সেটিং থেকে পরিবর্তন করতে হয়।
তাই আপনি সেটিং এ যান। সেখানে BBM Connected Icon এর মধ্যে টিক চিহ্ন উঠিয়ে দিন।

BBM লগ-আউটের নিয়মঃ BBM এর মাধ্যে সাভাবিক ভাবে লগ আউটের কোন অপশন নাই। যার জন্যে প্রথমে আপনার মোবাইলের সেটিংএ যান। সেখানে Apps/App Manager ক্লিক

করুন ও BBM কে তালাশ করে বের করুন। সেখানে Clear Data তে ক্লিক করুন। BBM একেবারে নতুন হয়ে যাবে এবং আপনি লগ-আউট হয়ে যাবেন।

মোবাইল রুট করার নিয়ম

মোবাইলে রুট / Root

রুটকে অন্য শব্দে ফ্লাশ বলে। অর্থাৎ এটা এমন পদ্ধতি যার মাধ্যমে কম্পিউটার দিয়ে মোবাইলকে ফ্লাশ দেয়া হয়। তারপরে মোবাইলের যাবতীয় অপারেটিং সিস্টেমকে নিজের ইচ্ছামত ব্যবহার করা যায়। এখন আমরা এমন একটি পদ্ধতির কথা বলব যা দিয়ে কম্পিউটার ছাড়া মোবাইল দিয়েই রুট করা যাবে। এবং এই পদ্ধতিতে কোন ধরনের ঝুকি নাই। অর্থাৎ এর মধ্যে লাইসেন্স বা অন্য কিছু করা লাগবে না। যখন ইচ্ছা রুটকে শেষ করে দিতে পারবেন। কিন্তু এভাবে রুট করার জন্য ইন্টারনেট আবশ্যক।

১/মোবাইলে রুট করার পদ্ধতিঃ-

এর জন্য একটি এপস ডাউনলোড করে ইইন্সটল করবেন, নাম kingroot। এটা নিয়মবহির্ভূত তাই গুগল প্লে স্টোরে পাওয়া যাবেনা। এর নতুন ভার্সনের লিংক: http://king.myapp.com/msoft/sec/secure/GodDresser/8/2/3/105203/NewKingrootV5.0.2_C167_B381_en_release_2017_01_12_20170112231602_105203.apk
আর যদি এর আপডেট ভার্সন চাই তাহলে এর ওয়েব সাইট দেখতে পারেন।
লিংক- http://www.kingroot.net

ডাউনলোড করে ইন্সটল করার পরে এটাকে ওপেন করলে এই লেখাটা দেখাবে Root Access not available অর্থাৎ আপনার মোবাইল রুট করা নয়। তখন এর Get now এই লেখাটার উপর ক্লিক করবে ৩-৮ মিনিট লাগতে পারে, কম বেশি হতে পারে। আর এটা নির্ভর করে ইন্টারনেট স্পিডের উপর। এই কাজ চলাকালীন ফোন এক দুইবার বন্ধ হয়ে নিজে নিজেই খোলতে পারে এতে পেরেশানির কোন কারন নাই।
এরপর যখন হয়ে যাবে তখন Root Saccessfully লিখা দেখাবে। এখন আপনার মোবাইল রুট হয়ে গেছে। ইন্টারনেট স্লো হলে একবারে নাও হতে পারে। তখন ২-৩বার চেষ্টা করতে

হবে। তখনও যদি না হয় তাহলে কম্পিউটারে চেষ্টা করেন। কম্পিউটারে রুট অনেক শক্তিশালী। আমরা সামনে তা নিয়ে আলোচনা করব ইনশাআল্লাহ।

ইউটিউব লিংক=
https://www.youtube.com/watch?v=1NVY17Zr2UQ
সরাসরি ডাউনলোড লিংক:-
https://archive.org/download/mobile_root_kingroot/mobile_root_kingroot.mp4

কম্পিউটার দিয়ে মোবাইল রুট

১/ কম্পিউটারের মধ্যে KingRoot সফটওয়্যার ডাউনলোড করবেন। KingRoot এর লেটেস্ট ভার্সন এই লিংক থেকে ডাউনলোড করা যাবে: https://kingroot.net
এখানে Download For Windows এর মধ্যে ক্লিক করে ডাউনলোড করে নিবে। এরপর ইন্সটল করবে। ইন্সটল হবে চাইনিজ ভাষায়। এতে পেরেশানির কিছুই নাই। শুধু নেক্সট চাপ দিয়ে ইন্সটল করে নিবে। বেশি জানার জন্য ভিডিও দেখে নিবে।

২/ মোবাইলের ড্রাইভারঃ- কম্পিউটারে মোবাইল ড্রাইভার সেটাপ দিবেন। ফলে মোবাইল যখন কম্পিউটারের লাগানো হবে তখন কানেক্ট হয়ে যাবে ইনশাআল্লাহ।

যদি মোবাইল স্যামসাং হয় তাহলে মোবাইলের মডেল এখানে তালাশ করে ডাউনলেড ও ইন্সটল করে নিবে- https://androidxda.com/download-samsung-usb-drivers

আর যদি মোবাইল Q হয় তাহলে এখান থেকে: https://androidxda.com/download-qmobile-usb-drivers

৩/ মোবাইলের মধ্যে USB Debugging কে Enable করবে। আর যদি মোবাইলের ভার্সন ৪.২ থেকে কম হয় তাহলে সিটিং থেকে Developer options এর মধ্যে যাবে। যদি Developer options আগ থেকেই অফ থাকে তাহলে প্রথমে অন করে নিবে। এরপরে USB debugging কে ok করে দিবে।

আর এন্ড্রয়েড ভার্সন ৪.২ থেকে ৫.১ হলে আর মোবাইলে Developer options না থাকলে তখন সিটিংয়ে যাবে। এরপর about phone এ যাবে। তারপর Build number কে ৮ থেকে ১০বার ক্লিক করবে। এর ভিতরেই you are now a developer লেখাটা আসবে। এরপর সেটিং এ ফিরে এসে Developer options এর উপর ক্লিক করবে। এরপর USB debuginng এর উপর ক্লিক করবে এবং Allow USB Debuginng কে ok করবে।

৪/শেষ পর্যায়: এখন Kingroot সফটওয়্যারকে ওপেন করবে ও মোবাইলকে কম্পিউটারের সাথে কানেক্ট করে নিবে। যদি সকল কাজ সঠিকভাবে হয়ে থাকে তাহলে এখন একটা স্ক্রিন আসবে যেটা চাইনিজ ভাষায়। অপশনকে ok করে দিবে এবং ডান দিকের অপশনটায় ক্লিক করবে। এখন মোবাইলের মধ্যে একটি অপশন আসবে সেটাকেও ok করে দিবে। এখন রুট হয়ে যাবে।

ভিডিও দেখে বুঝার জন্য ইউটিউব লিংক দেয়া হলো-
https://www.youtube.com/watch?v=MDWL19EMeKU

মোবাইল রুটের ঝামেলা নিষ্পত্তি

বর্তমানে অধিকাংশ নতুন এন্ড্রুয়েড ভার্সনে অথবা ভার্সণটি পুরানো হলে বিভিন্নভাবে ইডিট বা আপডেট করা হয়েছে, ফলে এই সকল মোবাইলগুলো রূট করতে সমস্যা হচ্ছে। আর এই সমস্যার কারণ হলো বর্তমানে মোবাইলের সিকিউরিটি আপডেট হওয়ার কারণে kingroot মোবাইল apps দ্বারা অধিকাংশ মোবাইল রুট হয় না।

এটা ব্যতিত kingoroot, Iroot, Root genius ইত্যাদি ধরণের apps রুট করার জন্য ব্যবহার না করা উচিত। এগুলোতে হ্যাকিংয়ের শিকার হওয়া এবং নজরদারিতে পড়ার ভয় থাকে। এসকল apps এর নির্মাতা অধিকাংশই চাইনিজ এবং এদের উপর কোনো ভরসা করা যায় না। কারণ তারা অধিকাংশ ক্ষেত্রেই গোয়েন্দা সফটওয়্যার মিলিয়ে দেয়। যার কারণে google playstore এ এই ধরণের apps রাখেনা।

গুপ্তচরবৃত্তি থেকে বাচার জন্য সবচেয়ে নিরাপদ পদ্ধতি হলো, PC মাধ্যমে রুট করে নেয়া এবং super su ইনস্টল করা। কিন্তু যেহেতু এই super su এর মাঝে সকল setup সঠিক ভাবে

দিতে না পারলে মোবাইল নষ্ট করে দেয় তাই আমরা এই পদ্ধতির কথা বলি না। কেননা এর জন্য দক্ষতার প্রয়োজন হয় এবং সামান্য ভুলের কারণে মোবাইল নষ্ট হওয়ার আশংকা রয়েছে।

যদি আপনি নিজের রিস্কে রুট করতে চান, তাহলে আপনি গুগলে আপনার মোবাইলের মডেল লিখে খোজ করুন যে, আপনার মোবাইলের মাঝে custom recovery কিভাবে ইনস্টল হবে? তারপর custom recovery এর প্রসিদ্ধ মাধ্যম যেমন, XDA, CWM, TWRP ইত্যাদি থেকে আপনার মোবাইলের জন্যে custom recovery ফাইল নামিয়ে ইন্সটল করে নিন। এরপর custom requery এর দ্বারা Super su কে আরামে ইনস্টল করতে পারবেন। এই পদ্ধতিগুলোও আপনি নিজের মোবাইলে গুগলে খোজ করে জেনে নিন। যখন এটা ইনস্টল করে নিবেন, তখন আপনার মোবাইল রুট হয়ে যাবে।

এই পদ্ধতি ইউজ করলে মোবাইলের ওয়ারেন্টি বাকি থাকেনা এবং পুনরায় নষ্ট হওয়ার আশংকা থাকে। কিন্তু আপনার নিরাপত্তাও জরুরি। কেননা বিভিন্ন প্রয়োজনীয় জিনিস ব্যবহার করার জন্য রুট আবশ্যক। এই জন্য রিস্ক নেয়া যেতে পারে। কেননা মোবাইল গেলে তো আরেক মোবাইল এসে যায়, কিন্তু মানুষ তো আর ফিরে আসেনা। এই জন্য নিজ জীবনের হেফাজত করা আবশ্যক।

পুরানো ব্যবহৃত মোবাইল অর্থাৎ সেকেন্ড হ্যান্ড মোবাইল ক্রয় করে এই ধরনের কাজের জন্য ব্যবহার করা যায় যাতে ভার্সন ৪ বা ৫ ইনিস্টল করা। সেগুলোতে এন্ড্রয়েড আপডেট অপশন বন্ধ করে পূর্বের নিয়ম অনুজায়ী অনায়াসে রুট করে নিতে পারবেন।

ফাইল পাঠানোয় ভাইরাস চেক

পিকচার, অডিও, ভিডিও, ডকুমেন্ট ফাইল, সফটওয়্যার পাঠানোর ক্ষেত্রে ভাইরাস চেক করা সম্পর্কে দিকনির্দেশনা।

বর্তমান সময়ে যেহেতু হ্যাকিং অতিমাত্রায় বৃদ্ধি পেয়েছে এবং যেকোন ফাইল এর সাথে ছোট থেকে ছোট কোন ভাইরাস অথবা নজরদারি কোন সফটওয়্যার ব্যবহার করে কারো মোবাইল অথবা কম্পিউটার হ্যাক করা হয়। এমনকি ডাটাও হাতিয়ে নেয়া হয়। এটা থেকে বাচার জন্যে অত্যন্ত জরুরি যে, আপনি যেই ফাইলটি আপনার সাথিদেরকে পাঠাচ্ছেন সে ফাইলটির প্রতি

তীক্ষ্ণ দৃষ্টি রাখা। যে উক্ত ফাইলের মধ্যে কোন প্রকার পরিবর্তন হয়েছে কি না? পরিবর্তন হওয়া বা না হওয়ার বিষয়টি চেক করার জন্যে উক্ত ফাইলের হ্যাশ কোড চেক করে নিশ্চিত হওয়া যে উক্ত ফাইলটি সেটিই যা আপনি আপনার সাথিদেরকে পাঠিয়েছেন , অথবা এবিষয়ে নিশ্চিত হওয়া যে উক্ত ফাইলটির মধ্যে কোন প্রকার পরিবর্তন সাধিত হয়েছে। এই ধরনের ক্ষতিকর ভাইরাসগুলো কোন পিডিএফ, ওয়ার্ড অথবা কোন সফটওয়্যারের সেটাপ ফাইলের সাথেও গোপন হয়ে চলে আসে।

হ্যাশ কোড চেক করার সময় বিভিন্ন হ্যাশ কোড আসে। নিম্নের কয়েকটি প্রসিদ্ধ হ্যাশ কোড:

SHA-1, S HA-256, MD5

এছাড়া নিম্নের গুলোও আসে:

SHA-384, SHA-512, SHA-3 ইত্যাদি।

এটার জন্য একটি সফটওয়্যার রয়েছে যার মাধ্যমে অতি সহজেই আপনি যে কোনো ফাইলের হ্যাশ কোড জানতে পারবেন। MD5 Sha1checksum utility সফটওয়্যার নিম্নের লিংক থেকে ডাউনলোড করতে পারবেন:

https://raylin.wordpress.com/downloads/md5-sha-1-checksum-utility
http://download.cnet.com/MD5-SHA-Checksum-Utility/3000-2092_4-10911445.html

এই সফটওয়্যারটি ব্যবহার করা একদম সহজ। প্রথমে উক্ত সফটওয়্যারটি ডাউনলোড করে ওপেন করুন। যে কোনো ধরনের ফাইল তাতে ড্রাগ-ড্রপ করে প্রবেশ করিয়ে দিন অথবা ব্রাউজ করে ওপেন করুন। এতটুকু কাজ আপনি সম্পাদন করলেই উক্ত সফটওয়্যারটি ফাইলের সমস্ত হ্যাশ কোড আপনাকে দেখিয়ে দিবে।

এখানে লক্ষনীয় বিষয় হলো ফাইলের নাম পরিবর্তন করার দারা তার হ্যাশ কোডের মধ্যে কোন প্রকার পরিবর্তন আসবেনা। ফাইলের হ্যাশ কোড শুধুমাত্র তার ভিতরে পরিবর্তন হওয়ার দ্বারা পরিবর্তন হবে চাই ফাইলের ভিতরে পরিবর্তন হওয়াটা সম্পাদনার মাধ্যমে হোক বা কম্পোজ করার মাধ্যমে হোক। এবং যখন আপনি সম্পাদনা বা অন্য কোনো কারনে ফাইলের মধ্যে অতি ছোট থেকে ছোট কোনো পরিবর্তন সাধন করবেন ঠিক তখনি হ্যাশ কোড পরিবর্তন হয়ে যাবে। সুতরাং এ বিষয়ের প্রতি লক্ষ রাখতে হবে যে আপনি যে ফাইল বা সফটওয়্যার পাঠাচ্ছেন তা যেন অপর জনের নিকট কোনো প্রকার পরিবর্তন ছাড়াই পৌছে। এর জন্য আপনি কোন একটি হ্যাশ কোড সংরক্ষণ করে আপনার সাথিকে পাঠিয়ে দিন যেন সে আপনার নিকট উক্ত কোডের সত্যায়ন করে। যেমন আপনি SHA-256 কোড নিয়ে কাউকে পাঠালেন

আর সে উক্ত কোডটি ঠিক আছে কি না তা চেক করলো , এর ব্যবহার পদ্ধতি আপনি শেষে দেয়ে ভিডিও লিংকে দেখতে পাবেন!

নোটঃ হোয়াটসঅ্যাপ এবং টেলিগ্রাম ইত্যাদি এপস্ এর মধ্যে যেহেতু অডিও, ভিডিও এবং পিকচার সম্বলিত ফাইলগুলো নিজে নিজেই সংকুচিত হয় এই জন্য তার ঐ হ্যাশ কোডটি বহাল থাকেনা যা প্রেরণ কারীর নিকটে থাকে , এছাড়াও আপনি উইন্ডোজের মধ্যে CMD/did অর্থাৎ ডোজের মাধ্যমে ফাইলের হ্যাশ কোড জানতে পারবেন , কিন্তু সফটওয়্যার পদ্ধতিই বেটার।

অনলাইনে ভিডিও দেখার লিংক, উর্দু
https://archive.org/details/HashTagSabaq
ভিডিও ডাউনলোড করার লিংক:-
https://archive.org/download/HashTagSabaq/Hash_Tag_Sabaq.mp4

এড বা বিজ্ঞাপনে ভাইরাস

প্রত্যেক ওয়েব সাইটেই বিজ্ঞাপন দেখতে পাবেন। যার মাধ্যমে তারা টাকা ইনকাম করে। কিন্তু আজকাল অনেক বিজ্ঞাপনের মধ্যে ম্যালাওয়ার ও ভাইরাস এড করা হয়। যার মাধ্যমে আপনি যখন বিজ্ঞাপনে ক্লিক করে তাদের সাইটে যাবেন তখন আপনার মোবাইল ও পিসিতে ম্যালাওয়ার, ট্রোজান বা ট্রেকার ইনস্টল হয়ে যাবে। যার ফলে সে আপনার তথ্য ও ডাটা চুরি করতে পারবে ও ব্রাউজারকে হ্যাক করে ফেলবে।

সম্ভবত আপনি শুরু থেকেই এর স্বীকার। যেমনঃ আপনার কখনো ব্রাউজারের সার্চ ইন্জিন নিজে নিজেই পরিবর্তন হয়ে যাবে, অথবা ব্রাউজার খুলার সাথে সাথেই বিজ্ঞাপন আসা শুরু হলো। এই ধরনের বিভিন্ন মাধ্যমে আপনার ব্রাউজার হ্যাকিং হতে দেখবেন। সবই ভাইরাস সম্বলিত এডের কারনে হয়।

গুগল কম্পানি শুধু ২০১৭ সালেই ১.৭ বিলিয়ন অথাৎ একশ সত্তর কোটি এড ব্লক করেছে যাতে ভাইরাস ও ম্যালাওয়ার ছিল। এটা হ্যাকারদের জন্যে আমাদের তথ্য হ্যাকিং এর সবচেয়ে সফল একটা মাধ্যম। কারন সব সাইটে টাকার বিনিময়ে এড প্রচার করে। অতপর তারা আমাদের তথ্য অন্যদের কাছে বিক্রি করে থাকে।

আজকাল ক্রিপ্টু মাইনিং এর জন্যেও এটা ব্যাবহার করা হয়। ক্রিপ্টু মাইনিং বুঝার জন্যে প্রথমে এটা জানুন যে, এখন ইন্টারনেটের টাকা তৈরি করা হয়েছে। যেগুলোকে গোপন টাকা বলা হয়। এগুলো মধ্যে সবচেয়ে প্রশিদ্ধ হচ্ছে বিট কয়েন। এখানে যে কেউ ঘরে বসেই নিজের কম্পিউটার বা গ্রাফিক কার্ড দিয়ে ক্রিপ্টু কারেন্সি বানাতে পারে। যাকে মাইনিং বলে। আর এই কাজকে ক্রিপ্টু মাইনিং বলে।

সুতরাং হ্যাকার আপনার পিসিকে তার আয়ত্বে নিয়ে ইন্টারনেটের টাকা আয়ের জন্য ব্যাবহার করে। সে সাধ্যের বেশি চাপ আপনার পিসির উপর প্রয়োগ করে এবং আয় করে। একই কাজ ইদানিং বিট টরেন্টের টরেন্সের মাধ্যমে করা হয়। ফায়দা ভোগ করে মূল ব্যাক্তিরা।

এই এড বা বিজ্ঞাপনের হামলা অনেক ব্যপক তাই এটাকে হালকা নিবেন না এবং অবশ্যই ব্লক করবেন।

১. এড ব্লক করার জন্যে ব্রাউজারে এডনস ইনস্টল করে নিবেন। যেমন ফায়ার ফক্স ব্যবহার করবেন। সেখানের জন্যেঃ

https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/

এবং এটাও

https://addons.mozilla.org/en-US/firefox/addon/noscript/

এই দুইটার মধ্যে ইউ ব্লক দিলে এড ব্লক হবে এবং নো স্ক্রিপ্ট দিয়ে স্ক্রিপ্ট ব্যবহারকৃত জিনিস ব্লক হবে।

আর কেহ যদি গুগল ক্রোম ব্যবহার করেন তো এখান থেকে ইনস্টল করে নিন।

https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en

ইহার জন্যে নোস্ক্রিপ্টের কোন প্লাগিন নাই। সবচেয়ে ভাল হবে যদি ক্রোম ব্যবহার না করেন।

২. ইহা ব্যাতিত আপনি কোন ভাল এন্টিভাইরাস ব্যাবহার করবেন। যা এই ট্রেকার ও এড ব্লক করবে।

৩. এড ব্লকের আরেকটা সফল সিস্টেম হচ্ছে ইন্টারনেট রাউটারে এমন ভিপিএন ব্যাবহার করবেন যা এড ব্লক করবে। এই ব্যাপারে বিস্তারিত ইন্টারনেটে সার্চ করে নিতে পারেন।

শর্ট লিংকে ভাইরাস

হ্যাকাররা লিংক শর্ট করার মাধ্যমগুলোকে ভাইরাস জনিত লিংক ছড়িয়ে দেয়ার কাজে ব্যবহার করে। অর্থাৎ ভাইরাসের লিংককে ছোট করে ফলে সেটা শর্ট লিংকের মত দেখায় এবং যাতে ব্যবহারকারী সন্দেহ না করে। ভিপিএন বা টর ব্যবহারের মাধ্যমে IP পরিবর্তন না করলে ভাইরাস জনিত শর্ট লিংকে একবার ক্লিক করা ফলেই আপনার অবস্থা প্রকাশ হয়ে যাবে। ইন্টারনেটে ট্র্যাকিংইয়ের জন্যে অধিকাংশরাই এই মাধ্যম প্রয়োগ করে।

শর্ট লিংক যাচাইয়ের পদ্ধতি

১/ virustotal.com এই সাইটে প্রবেশ করুন > খালী ঘরে URL পেস্ট করুন > Scan ক্লিক করুন। যদি প্রত্যেকটা ঘরে সবুজ হয় অর্থাৎ 67/0 হয় তাহলে নিরাপদ। আর যদি একটাতেও লাল চিহ্ন থাকে তো নিরাপদ নয়।

২/ unfurlr.com সাইটে প্রবেশ করুন > লিংক পেষ্ট করে Check it ক্লিক করুন। এখন আপনাকে মূল লিংকটা ও কোন পিসি দিয়ে কোন জায়গা থেকে করা হয়েছে তাও দেখাবে।

৩/ getlinkinfo.com সাইটে প্রবেশ করুন > লিংক পেষ্ট করে Get link info তে চাপ দিন। যদি সব safe আসে তো নিরাপদ।

থ্রিমা মেসেঞ্জার এপস

খুবই ভাল একটা মেসেঞ্জার এপস। এতে আইডি বানানোর জন্য কোন মোবাইল নাম্বার, ইমেল আইডি বা ভেরিফাইয়ের প্রয়োজন হয়না। এই এপসের বিশেষ একটি জিনিস হলো তার সিকিউরিটি খুবই শক্তিশালী। সকল চ্যাট ও যোগাযোগ ইনক্রিপ্ট (কোডের মাধ্যমে) হয়ে যায়। আইডি বানানো খুবই সহজ। এর দ্বারা চ্যাট করা যায়। ভিডিও, অডিও ও পিকচার পাঠানো যায়।

ভিডিওর মধ্যে এপসকে ডাউনলোড করা, আইডি বানানো, এপসকে অনেক নিরাপদ রাখার জন্য সিটিংস, অন্য কারো সাথে আইডি এড করার পদ্ধতি, মেসেজ করা, মেসেজ ও সকল হিস্টরি ডিলেট করার পদ্ধতি উর্দু ভাষায় খুবই সহজ করে বুঝানো হয়েছে।

(বাংলাদেশে আইএসে গুলশান হামলার পরে থ্রীমা এপ ব্যবহারের প্রমান থাকায় ত্বাগুত বাহিনী এই দেশে থ্রীমা ব্লক করে দিতে চেয়েছিল। ফলে ভিপিএন কানেক্ট দেয়া ছাড়া এই দেশে থ্রীমা আইডি বানানো, অন্য আইডি এড করা যায় না ও মেসেজিং ঝামেলা হয়। তাই সর্বদা ভিপিএন সহ ব্যবহার করুন।)

ভিডিও দেখার জন্য এই লিংক:
https://www.faecbook.com/1625527211086231/videos/1625528344419451/

USB শর্টকাট ভাইরাস

আজকাল ইউএসবিতে ভাইরাস ব্যাপক আকার ধারন করেছে। যার কারনে USB তে ফোল্ডারগুলো শর্টকাট হয়ে যায় আর মূল ফোল্ডার হাইড হয়ে যায় বা ফোল্ডারের ফরমেট পরিবর্তন হয়ে এপ্লিকেশন ফরমেটে পরিনত হয়।

অধিকাংশ লেপটপ বা কম্পিউটার এর দ্বারা প্রভাবিত হয়। অধিকাংশ এন্টি ভাইরাস এগুলোকে পরিপূর্ণ ভাবে ধংস করতে পারেনা। যার কারনে এন্টি ভাইরাসের প্রভাব থেকে যায়। এরপর সেই কম্পিউটারে নতুন কোন USB লাগালে সেখানেও সেই ভাইরাস স্থানান্তরিত হয়। এভাবে ভাইরাস ব্যাপক ভাবে ছড়িয়ে পড়ে। পুরাতন ভার্সনগুলো এখনো এন্টি ভাইরাসের নিয়ন্ত্রনে আছে। কিন্তু ইদানিং নতুন ভার্সনগুলোতে ভাইরাস তৈরী কারীরা আরো মজবুত ভাবে তৈরী করছে। এর একটা চূড়ান্ত সমাধান আমরা আলোচনা করব ইনশাআল্লাহ।

১। USB Fix এই সফটওয়ার ডাউনলোড করুন ৩/৪ এমবির মধ্যেই হয়ে যাবে। ডাউনলোড লিংক

https://www.fosshub.com/UsbFix.html

২। ইনস্টল করার পর আপনার ভাইরাস আক্রান্ত USB লেপটপে লাগান। এর পর সেই সফটওয়ারের clean অপশনে ক্লিক করুন। এতে কয়েক মিনিটের মধ্যেই আপনার লেপটপ এবং ইউএসবি ভাইরাসকে ধংস করে দিবে ইনশাআল্লাহ।

নোট : এই সফটওয়ার কোন এন্টি ভাইরাস সফটওয়ার নয় এটা শুধু USB ভাইরাসের জন্য।

প্রাসঙ্গিক টিপস : এন্টি ভাইরাস আপনি কেন ব্যবহার করবেন? একটি ভালো এন্টি ভাইরাস নির্বাচনই আপনাকে হ্যাকিং থেকে নিরাপত্তা দিতে পারে। এন্টি ভাইরাস ছাড়াও মাইক্রোসফটের একটি ফ্রী সফটওয়ার আছে যা মালওয়্যার এবং স্পাইওয়্যার থেকে নিরাপত্তা দিবে। Malicious Software Removal Tool এর লিংক হচ্ছে:

https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx

এই সফটওয়ার ডাউনলোড করুন। এবং এর মাধ্যমে প্রতি সপ্তাহে একবার আপনার কম্পিউটার স্কেন করুন। এটা মালওয়্যার এবং স্পাইওয়্যার অর্থাৎ গোয়েন্দা সফটওয়ারের বিপরীতে কাজ করে।

এটা ইনস্টল করার প্রয়োজন নেই বরং ইনস্টল ছাড়াই এটা কাজ করে। যার ফলে আপনার ডিভাইসে হালকা বা ভারী কোন হেরফের হবেনা। আর প্রত্যেকবার যখন আপনি স্ক্যান করবেন তখন দুইবার করে স্ক্যান হবে। তবে এটাও স্বরন রাখবেন যে এটা পরিপূর্ণ কোন এন্টি ভাইরাস নয়। বরং এটা এন্টি ভাইরাসের সহায়ক। এটাকে অন্য এন্টি ভাইরাসের সাথে ব্যবহার করা চাই।

নোট: এই মাইক্রোসফট এন্টি মালয়্যার প্রত্যেক উইন্ডোজের জন্য আলাদা ভার্সন আছে। লিংকে যখন আপনি আপনার ব্রাউজারে সার্চ দিবেন তখন এটা স্বয়ংক্রিয় ভাবেই আপনার উইন্ডোজ ডিটেক্ট করে নিবে। অবশ্য একটা কথা মনে রাখবেন আপনি এই ফাইল আপনার ইচ্ছা অনুযায়ী সাধারন কোন ব্রাউজার দিয়ে অথবা টর দিয়ে ডাউনলোড করতে পারেন।

কিন্তু যদি উইন্ডোজ ৮ অথবা ১০ এর ব্যবহারকারীকে টর ব্রাউজারে উইন্ডোজ ৭ এর টা দেয় তাহলে সাধারন ব্রাউজার দিয়ে ঐ লিংক খোলে ফাইল ডাউনলোড করে নিবেন যাতে উইন্ডোজ অনুযায়ী ডাউনলোড মিলে যায়।

সার্চ ইঞ্জিনের নিরাপত্তাঃ ঝুকি ও সমাধান

Google এর সেবাগুলো ব্যবহার না করার জন্য আমরা পূর্বে বলেছি। তাই সেই ধারাবাহিতায় এর বিকল্প বলে দেয়া জরুরি। এই বিকল্প আগেও বলা হয়েছে। কিন্তু এখন খুব গুরুত্বের সাথে বলা হচ্ছে এবং এই কথাকে গুরুত্বহীন ভাবা যাবেনা। কেননা Google আপনার ব্যপারে গোয়েন্দাগিরি করতে কোন প্রকার ত্রুটি করবেনা।

১/ Google chrome - কিছুদিন আগে একটা রিপোর্ট এসেছে যে Google chrome এর একটা টুল আছে - ক্লিনাব টুল - যা আপনার ফাইলগুলোকে স্ক্যান করতে থাকে। এবং প্রয়োজন হলে বলেও দিতে পারবে যে আপনার কম্পিউটারের মধ্যে ভাইরাস আছে। Google chrome এর কাজ তো শুধু ব্রাউজিং, এটার এন্টিভাইরাসের কাজ করার কী প্রয়োজন!!!!! Google কোম্পানী বলে যে এর দ্বারা তারা দেখতে চায় কোন সফটওয়্যার বা ফাইল ক্রোমের জন্যে বাধাদানকারী। তবে বাস্তব কথা হলো তাদের উদ্দেশ্য আপনার ডাটাকে বাজেয়াপ্ত করা ও গোয়েন্দাগিরি করা। এই জন্য Google chrome কে ব্যবহার না করে ফায়ারফক্স ব্যবহার করবেন। এটা একটা ভালমানের বিকল্প।

২/ Google search - এর মধ্যে কোন সন্দেহ নাই যে গুগল সবচে ভাল সার্চ ইঞ্জিন। কিন্তু এটা সার্চের মাধ্যমে আপনার চিন্তা, আগ্রহ ও দর্শনের সাথে সম্পৃক্ত বিভিন্ন তথ্যাদি জমা করে রাখে। যাতে পরবর্তিতে ইন্টিলিজেন্স কম্পানিকে এই তথ্যাদি দিতে পারে। তাই গুগল সার্চ ইঞ্জিন ব্যবহার না করা উচিত। তবে এই কথা স্বরণ রাখা উচিত যে গুগলের বিকল্প হিসাবে আমরা যা বলব তা বাহ্যিকভাবে গুগলের বিকল্প হওয়ার যোগ্য না। তবে সিকিউরিটি ও প্রাইভেসি রক্ষার জন্য কিছু বিকল্প উল্লেখ করা হবে ইনশাআল্লাহ।

গুগল সার্চ ইঞ্জিনের বিকল্প:

১/ startpage - এটাই সবচে ভালমানের বিকল্প। এটা স্বয়ং গুগল search মাধ্যমই তবে ট্রাকিং ছাড়া ও সোর্স স্টার্ট পেইজ থেকে হবে।। এটা আপনাকে সরাসরি গুগল থেকে ফলাফল এনে দিবে কিন্তু গুগল আপনার সম্পর্কে কিছুই জানতে পারবে না। অর্থাৎ আপনার প্রাইভেসি ঠিক থাকবে।

এটাকে সেট করার জন্যে এর ওয়েবসাইটের মধ্যে যাবেঃ https://www.startpage.com/ এর শুরুতেই এই লেখা আসবে add to firefox বা আপনার ব্রাউজারের নাম আসবে। তখন এটাতে ক্লিক করলে আপনার ব্রাউজারের মধ্যে এই সার্চ ইঞ্জিন ইন্সটল হবে।তারপর সিটিংস থেকে তাকে সিলেক্ট করে নিবে।

২/ qwant - এটাকে ইন্সটল করার জন্য এটার ওয়েবসাইটের মধ্যে যাবেন ও এবং এর মধ্যে ইন্সটল ক্বাউন্টের উপর ক্লিক করবে এবং এড করে নিবেন। https://www.qwant.com/

৩/ disconnect - এটাও স্টার্ট পেইজের মত নিজে সার্চ করেনা। বরং ডাক ডাক গো বা ইয়াহুর মাধ্যমে সার্চ করে। প্রাইভেসিকে ঠিক রেখে নিজস্ব মাধ্যমে আপনার সামনে উপস্থিত করবে। https://search.disconnect.me/

৪/ searx - এটাও অনেক ভাল সার্চ ইঞ্জিন। তবে ব্রাউজারের জন্য এর ভাল কোন প্লাগিন পাওয়া যায়নি এখনো। যার ফলে এটার অয়েব সাইটকেই বারবার ভিজিট করতে হবে তাই আমরা এটাকে ৪ নাম্বারের উল্ল্যেখ করেছি। অন্যথায় এটাও সিকিউরিটির দিক থেকে অনেক ভাল এবং ওপেন সোর্স মাধ্যম। https://searx.me/

চেষ্টা করবেন startpage বা ক্বাউন্ট ব্যবহার করার জন্য। duckduckgo এর ব্যপারে অনেকে ব্যবহার করার মাশওরাহ দিয়ে থাকেন। এমনকি আমরাও প্রথমে এটা ব্যবহারের মাশওয়ারাহ দিতাম। তবে সেটার ব্যপারে আমাদের গবেষনা ছিলনা। তাই আগের কথা থেকে আমরা ফিরে আসলাম।

ডাক-ডাক-গু কম্পানি ইয়াহু, আমাজন ও আইবি মত সন্দেহজনক কম্পানির সাথে সম্পৃক্ত। এর প্রাইভেসি পলিসিও অন্যান্য গোয়েন্দা কম্পানির চেয়ে কোন অংশে কম নয়। এই

কম্পানিও বলেছে যে আমরা ডাটা জমা রাখি, সার্চ করা শব্দাবলীও জমা রাখে। এছাড়াও আইপি এড্রেস ও অন্যান্য তথ্যাদি নিজের কাছে জমা রাখে। অর্থাৎ সেই সোর্সের ব্যবহারও উপযোগী না।

কোন সিকিউরিটি অভিজ্ঞ ব্যক্তির কাছ থেকে হয়ত এটার অনুমতি হয়েছিল। পরে সবাই কোন প্রকার গবেষনা ছাড়াই অনুমতি দিতে ছিল। একপর্যায়ে বিষয়টা এই পর্যন্ত গড়িয়েছে যে প্রত্যেকেই গুগলের বিকল্প হিসাবে ডাক-ডাক-গু এর মাশওরাহ দেয়। মোটকথা এখন এটা থেকে বিরত থাকতে হবে।

IDM কে টর কানেক্ট

যখন ব্রাউজিংয়ের জন্য টর ব্যবহার করা হবে এবং এর থেকে লিংক দিয়ে যে কোন ডাউনলোড ম্যানেজারের মাধ্যমে কোন কিছু ডাউনলোডের সময় যদি ভিপিএন ব্যবহার না করা হয় তাহলে সেই ফাইল সাধারণ ট্রাফিক থেকে ডাউনলোড হবে। ফলে এটা নিরাপদ থাকবে না। কেননা যে পরিচালনা বিভাগ ইন্টারনেট ট্রাফিক নজরদারি করে তারা অবশ্যই বুঝতে কী ডাউনলোড হচ্ছে।
ভিপিএন ব্যবহার করা ছাড়া যদি শুধু টর ব্যবহার করেন আর কোন জিনিস ডাউনলোড করা প্রয়োজন হয় তাহলে ডাউনলোড ম্যানেজারকে টর নেটওয়ার্কে চালিয়ে ডাউনলোড করবেন। তখন কোন ভিপিএন ব্যবহার করার প্রয়োজন হবে না।

ইন্টারনেট ডাউনলোড ম্যানেজারকে টর নেটওয়ার্কের সাথে চালানোর জন্য প্রথমে ইন্টারনেট ডাউনলোড মেনেজারকে ওপেন করুন। এবং অপশনে যান। সেখানে proxy/socks ট্যাবের মধ্যে যান। এরপর use socks অপশনকে ok করে দিবেন। এখন এই অপশনের নিচে prot ঘরে 9150 লিখে ok করে দিবে। এবং ইন্টারনেট ডাউনলোড মেনেজারকে বন্ধ করে দিবেন। এরপর প্রথমে টর ব্রাউজার খোলে পরে ইন্টারনেট ডাউনলোড মেনেজার ওপেন করুন। এখন আপনি যা কিছুই ডাউনলোড করবেন সব কিছু টর নেটওয়ার্কের মধ্য দিয়েই ডাউনলোড হবে।

নোটঃ এই কাজ সম্পন্ন হওয়ার পর টর নেটওয়ার্ক ছাড়া ইন্টারনেট ডাউনলোড মেনেজার কোন কাজ করবেনা। ফলে টর চালানো জরুরি হয়ে যাবে। এখন কেউ যদি নরমাল ট্রফিক দিয়ে ডাউনলোড করতে চায় তাহলে use socks গিয়ে টিক উঠিয়ে দিবে।

সোশ্যাল মিডিয়া ব্যবহারে সতর্কতা

সোশ্যাল মিডিয়া ব্যবহার বিশেষ করে ফেসবুক ব্যবহার না করাই সবচেয়ে উত্তম। কারন বর্তমানে ফেসবুক রীতিমতো একটি গুয়েন্দা মাধ্যম। সে ক্যামেরার মাধ্যমে ব্যক্তিকে দেখা এবং আওয়াজ শুনার আন্তর্জাতিক অনুমোদন পেয়েছে। অর্থাৎ নিকট ভবিষ্যতে এমনকি বর্তমানেও সে এই কাজগুলো করে যাচ্ছে।

এখন যদি আপনি ফেইসবুক ব্যবহার করতেই চান যে আপনি এর মাধ্যমে দাওয়াতি কাজ করবেন তাহলে এই সতর্কতা মূলক পদক্ষেপগুলো অবলম্বন করুন।

কিছু পদক্ষেপ আছে যেগুলো নিজের নিরাপত্তার জন্য আর কিছু আছে একাউন্ট দ্রুত ব্লক হওয়া থেকে রক্ষা করার জন্য।

১। আপনি ফায়ার ফক্স ব্রাউজার ব্যবহার করবেন। এবং এর মধ্যে কুকিজ এবং হিস্ট্রি সংরক্ষন করবেননা। এর পদ্ধতি হলো আপনি সিটিংয়ে Privacy and security ট্যবের মধ্যে History তে Never remember history সিলেক্ট করুন।

তাছাড়া আপনি ফায়ার ফক্সের Private window খোলতে পারেন। এর পদ্ধতি হলো আপনি ব্রাউজারের মেনুতে গিয়ে New Private window তে ক্লিক করবেন। এর মাধ্যমে আপনার ব্রাউজার তার হিস্ট্রি, পাসওয়ার্ড, কুকিজ, টেম্পরারি ফাইলস ইত্যাদিকে সংরক্ষন করবে না।

২। ফেসবুকের জন্য টর ব্রাউজার ব্যবহার করবেন না। বরং এমন ভিপিএন ব্যবহার করবেন যার মাধ্যমে একই দেশের আইপি থেকে লগ অন হয়। কারন টরের মধ্যে আপনার আইপি বিভিন্ন দেশে বদলাতে থাকে। যার কারনে আপনার আইপি ফেসবুকের নজরে সন্দেহ সৃষ্টি করে যা ফেসবুক আইডি দ্রুত ব্লক হয়ে যাওয়ার কারন হয়।

৩। কাজ শেষ হওয়ার পরপর লগ আউট করে দিবেন। কারন আপনি যদি লগ ইন করে নেটে কোন কিছু দেখতে থাকেন তাহলে সে আপনার অবস্থা নিজের কাছে সংরক্ষন করে যে আপনি কী দেখছেন।

৪। ফেসবুক এপ ব্যবহার করবেননা শুধু ব্রাউজার দিয়েই চালাবেন।

৫। একই একাউন্ট দিয়ে আপনি সকল শ্রেনীর লোকদেরকে ফ্রেন্ড বানাবেন না। প্রত্যেক শ্রেনীর লোকদের জন্য আলাদা একাউন্ট হবে। এবং এর মধ্যে কোন মিউচুয়াল ফ্রেন্ড থাকবে না। এমনি ভাবে একই নাম ব্যবহার করবেন না বরং প্রত্যেক একাউন্টের জন্য আলাদা নাম রাখবেন।

৬। ফ্রেন্ড কম রাখবেন এবং ফলোয়ার বাড়াবেন।

৭। কোন পার্সনাল বিষয় প্রকাশ করবেন না। এবং নিজের পরিচিত কোন ছবি চাই সেটা কোন কমান্ডারের ছবি হোক বা কোন জায়গার ছবি হোক যেটা আপনি তুলেছেন।

৮। ফেসবুক আইডিতে কখনো কোন গোপন কথা বলবেন না। কোন কাজের প্লানিং বা রেকির ব্যপারে কোন কথা সেখানে বলবেন না।

৯। যদি সম্ভব হয় তাহলে কোন নেক মানুষের ছবি নেট থেকে অথবা অন্য কোথাও থেকে সংগ্রহ করে আপনার প্রোফাইলে লাগিয়ে দিন।

১০। যদি মোবাইল দিয়ে লগ ইন করেন তাহলে চেষ্টা করবেন ফায়ার ফক্স ব্যবহার করতে অথবা ডাক ডাক গু ব্রাওজার ব্যবহার করবেন। এবং সেই ব্রাউজারের ক্যামেরা এবং লোকেশন পারমিশন দিবেন না।

১১। চেষ্টা করবেন মোবাইলটা এন্ড্র*য়েডের নতুন ভার্সন নিতে যার মধ্যে পারমিশন দেওয়া না দেওয়ার বিষয়টা আপনার হাতে থাকে।

১২/ বিশেষভাবে আরেকটা জিনিস খেয়াল রাখবেন আজকাল মোবাইলে যে সমস্ত সুবিধা দেওয়া হয় যেমন ফিঙ্গার প্রিন্ট, ফেইস আনলক ইত্যাদি ব্যবহার করবেন না।

১৩/ ফেইসবুকের ব্যপারে কিছুদিন আগে একটা খবর এসেছিল। বলা হয়েছিল যে, ফেইসবুক

এখন মোবাইলের ক্যামেরা ও লেপটপের সামনের ওয়েব ক্যামেরার মাধ্যমে ব্যবহারকারীদের সবকিছুই দেখতে পারে। ফলে তারা এটা বুঝে নিতে পারে তাদের কোন পোষ্ট ভাল লাগছে আর এটাকে বেশির চেয়ে বেশি দেখাতে পারে। অথবা যে সমস্ত এড তারা দেখাতে থাকে। তখন তাদের চেহারার অসন্তুষ্টি দেখে বুঝা যাবে কোন পোষ্ট তাদের ভাল লাগে নি। ফলে সেই পোষ্ট তার সামনে আসবেনা। যার মধ্যে মাকসাদ এটা থাকে যে ব্যবহারকারীরা অনেক বেশি ফেইসবুক ব্যবহার করতে থাকে।

তারা সেই টেকনোলোজি পেটেন্ট অর্থাৎ কপিরাইট নিজের জন্য সংরক্ষিত রাখে। এটা বাহ্যিক উদ্দেশ্য হচ্ছে আপনার পর্দা লঙ্ঘন হচ্ছে, আপনার উপর গুপ্তচরবৃত্তি করা এবং আপনার ব্যপারে বিভিন্ন তথ্য জমা করে রাখা। অভিজ্ঞ ব্যক্তিরা এটা নিয়ে আরো ফিকির করবেন। বাকী আল্লাহই ভাল জানেন।

এই কারনে কিছু সচেতনমুলক পরিকল্পনা গ্রহণ করা জরুরিঃ-

ক/ ফেইসবুক এপ বা যে ব্রাউজার দ্বারা ফেইসবুক চালানো হচ্ছে সেটার ক্যামেরার পারমিশন না দেয়া। এন্ড্রয়েট 6 ভার্সনের মধ্যে এই কাজ খুব সহজেই করা যাবে। কিন্তু এর পুরাতন ভার্সনগুলোর মধ্যে এটা করার জন্য মোবাইলকে রুট করা জরুরি। যাতে এই পারমিশনকে প্রতিহত করা যায়।

(রূটের পদ্ধতি আমরা পূর্বের পাঠে আলোচনা করেছি। যার প্রয়োজন হবে সে আমাদের টেলিগ্রামের পুরাতন পাঠ দেখে নিবে।)

খ/ যদি আপনার জন্য এটা করা কঠিন হয় তাহলে এই পদ্ধতি অবলম্বন করুন, মোবাইলের সামনের ক্যামেরায় এমন কোন জিনিস দিয়ে বন্ধ করে দিন যার কারনে তারা আপনাকে দেখতে পারবেনা, কোন মার্কার দিয়েও তা করা যায়। টেপ বা অন্য কিছুও লাগানো যায়।

গ/ যদি আপনি লেপটপ ব্যবহার করেন তাহলে ব্রাউজারের সিটিংসের মধ্যে সর্বদা ক্যামেরার পারমিশন অফ রাখবে। (এর তরিকাও আলোচনা করা হয়েছে। যে ভাল করে জানতে চাই সে আগের আলোচনা দেখে নিবে)

লেপটপের ওয়েবক্যমেরার মধ্যেও কোন কিছু লাগিয়ে দিবে।

অধিকাংশ বিশেষজ্ঞরা এমনকি ফেইসবুকের প্রতিষ্ঠাতা মার্ক যাকার্বার্গ লেপটপের ওয়েবক্যামেরার উপর টেপ লাগিয়ে রাখে যাতে যদি তার উপর গোয়েন্দাগীরি করতে চাইয় তাহলে যেন সে তাদের নজরদারিতে না আসে। যেটা আপনি এই লিংকে দেখতে পারবেনঃ

http://www.anonews.co/wp-content/uploads/2016/06/zuck_431106.png

এই ব্যপারে কেউ যদি আরো বেশি জানতে চাই তাহলে এই ইংরেজিতে এই খবরের লিংকটা দেখতে পারেন।

http://www.cybersecurity-insiders.com/facebook-to-spy-througt-your-webcam-or-phone/

http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-plans-to-watch-users-through-webcams-spy-patent-application-sociol-media-a777911.htm

১৪/ ফিশিং ওয়েবসাইট থেকে বেচে থাকাঃ-

এখন হ্যাক অনেক ব্যপক হয়ে গেছে। আর লোকেরা এই ব্যপারে কিছু না জানার কারনে হ্যাকের শিকার হচ্ছে। তাই আমারা হ্যকিংয়ের ব্যপারে সবাইকে ভিত্তিমূলক বিষয়গুলো জানাব আর তাদেরকে হ্যাক থেকে বাচার তরিকা বলে দিব। যাতে শত্রুর আগ্রাসন থেকে বাচার জন্য সচেতনমুলক পদক্ষেপ নিয়ে নিরাপদ থাকতে পারে। এই ব্যপারে আমরা অতিরিক্ত আলোচনা করব না। শুধু তরিকাটা বলব যা এখন শত্রুরা ব্যবহার করে।

এর মধ্যে সবচে পুরাতন তরিকা হলো phishing ফেশিংয়। যেটা ২০০৫ সালে কোন এক সময় ঝাকঝমক ছিল। কিন্তু লোকেরা যখন এর ব্যপারে জেনে গেল তখন এটা অকেজো হয়ে যায় এবং এর ব্যবহারও বন্ধ হয়ে যায়। কিন্তু আমাদের দেশের মানুষ যেহেতু ইন্টারনেট বেশি পরিমানে ব্যবহার শুরু করেছে কয়েক বছর হয়েছে।আর মানুষও এই ব্যপারে ধারনা শুন্য। তখন শত্রুরা এর ফায়েদা নেয়ার জন্য পুরাতন পদ্ধতি অবলম্বন শুরু করে দিল।

ফিশিং:-

এর অর্থ অনেক ব্যপক। যার উদ্দেশ্য হলো, যাকে হ্যাক করবে তার সত্তাগত পরিচয় বের করা। যথা ক্রিডিট কার্ডের নাম্বার, ফোন নাম্বার। কারো আইডির নাম ও পাসওয়ার্ড ইত্যাদি। কিন্তু আমাদের আলোচ্য বিষয় এখন ক্লোন ফিশিং ওয়েবসাইট। যার উদ্দেশ্য হলো, আক্রমণকারীর আইডি, পাসওয়ার্ড নেয়া। (যেমন ফেইসবুক, জিমেইল, ইয়াহু ইত্যাদি) এই কাজটাকে সম্পন্ন

করার জন্য হুবহু আসল ওয়েবসাইটের মত একটা নকল ওয়েবসাইট বানায়। এরপর সেটার লিংক পাঠিয়ে দেই। এটার মধ্যে ইউজারনেম ও পাসওয়ার্ড তলব করবে। অর্থাৎ যখন সেই নকল লিংকটা খোলা হবে পুরাপুরি আসল লিংক খোলার মতই খোলবে। এখন আমরা আরো সহজ ভাষায় বুঝানোর চেষ্টা করব উদাহরণ দিয়ে। সাধারণত আসল ফেইসবুকে লিংকে যেভাবে ইউজারনেম ও পাসওয়ার্ড দেয়া হয়।

(ফেইসবুক আসল লিংক https://www.facebook.com বা https://m.facebook.com) ঠিক তেমনিভাবে নকল ফেইসবুক লিংকে ইউজারনেম ও পাসওয়ার্ড চাবে। যখন ইউজারনেম ও পাসওয়ার্ড দেয়া হবে তখন পাসওয়ার্ড ও আইডি হুবহু শত্রুর কাছে চলে যাবে। এরপর শত্রু পাসওয়ার্ড পরিবর্তন করে নতুন পাসওয়ার্ড লাগিয়ে দিবে। এবং এই একাউন্টের উপর পুরা কর্তৃত্ব করবে। অথবা পাসওয়ার্ড পরিবর্তন করবে না আগেরটাই রেখে দিবে যাতে সন্দেহ না হয়। আর এই আইডিকে ব্যপকভাবে ব্যবহার করবে। এবং হ্যাক করা ইউজারনেম ও পাসওয়ার্ডকে তারা ব্যবহার করে নজরদারি করতে থাকবে এই আইডি দিয়ে কার সাথে কী কথা হয়। আর এটা করার আগে দীর্ঘ সময় তারা বন্ধুত্ব দেখাবে।নিজেদেরকে মুজাহিদ হিসাবে প্রকাশ করবে। অথবা আপনি যে বিষয়ে পারদর্শী সে বিষয়ে আপনার সাথে কথা বলে বন্ধুত্ব করে নিবে।যাতে বিন্দু পরিমাণ তাদের প্রতি সন্দেহ না থাকে। আর তাদের দেয়া লিংক ব্যবহার করা হয়। অথবা তাদের লিংককে সামনে দেখাবে আর বলবে এটা আমাদের পেইজ। সুতরাং লাইক কর। এভাবে তারা আপনার সবকিছুকে রেকর্ড করবে।

বাচার পদ্ধতিঃ-

এর থেকে বাচা অনেক সহজ। শুধু দেখে নিবেন আপনি যে লিংক খোলছেন (আইডি, পাসওয়ার্ড চাচ্ছে) সেটা আসল নাকি নকল।অর্থাৎ সেগুলো নিচে দেয়া দুইটা লিংকের মত হবে। প্রথমটা যারা কম্পিউটার চালায় তাদের জন্য। আর দিতীয়টা মোবাইল যারা চালায় তাদের জন্য।
https://www.facebook.com বা https://m.facebook.com সুতরাং উপরে দেয়া দুইটা লিংক ছাড়া অন্য কোন লিংক যদি হয় তাহলে বুঝে নিতে হবে এটা ফিশিং সাইট।

ফিশিং সাইট কিভাবে হয়ঃ-

এজেন্সির লোকদের প্রসিদ্ধ একটা ফেশং সাইট আছে যার দারা মুজাহিদদেরকে ধোকা দেয়: http://talibislam.somee.com/?fbid=934448985285672886 11&set=a.763335483356816.08379.981729056298491&type=1&relevant_count=1&ref=nf

আসল লিংক এটা: http://talibislam.somee.com ধোকা দেয়ার জন্য তারা অনেক বড় লিংক দিয়ে থাকে যাতে সন্দেহ না হয়। তো এটার মধ্যে দেখা যাচ্ছে যে এটা ফেইসবুক ওয়েবসাইট নয়। বরং একটা ফিশিং সাইট। আবার কখনো এমনও হয় যে, হুবহু ফেইসবুকের মতই লেখা হবে।অর্থাৎ শব্দগুলো ফেসবুকের মত হবে।উদাহরণসরুপ নিচের দুইটা লিংক দেখে নেন যে হুবহু ফেইসবুকের মত। http://www.fecebock9.tk বা http://www.fasebo0k.wapka.me এই দুইটাও ফিশিং সাইট যা ফেইসবুকের নামে ধোকা দেয়ার জন্য বানানো হয়েছে। কিন্তু একটু ফিকির করলেই স্পষ্ট বুঝা যাবে যে এগুলো ফেইসবুক সাইট নয়, এই জন্য নকলগুলো থেকে সাবধান!!!!!

সুতরাং ভালভাবে আগে শব্দগুলো দেখে নিতে হবে। এবং যদি এরকম সাইট আসে তাহলে কখনো লগইন করা যাবেনা। অথবা পরিক্ষা করার জন্য ভুল আইডি ও পাসওয়ার্ড দিবে আর দেখবে কী হয়! সাধারণত অন্য আরেকটি পেইজ খোলে বা ফেইসবুকের আসল লগইন পেইজ খোলে। অথবা অন্য কোন কিছু আসতে পারে।

এখন অতিতে যদি এই সমস্যার সম্মুখীন হয়ে থাকেন তাহলে খুব দ্রুত আপনার একাউন্ট ও পাসওয়ার্ড পরিবর্তন করতে হবে। বর্তমানে ফিশিং সাইট বানানো খুব সহজ। এটা কোন হ্যাকিং ফোরাম থেকে সহজেই ফাইল পাওয়া যায়। এটাকে বিনামূল্যে ওয়েব হুস্টিংয়ের উপর আপলোড করবে। এবং এর লিংক লোকদেরকে দিয়ে দিবে যারা এর মধ্যে লগইন করবে। তার ইউজারনেম ও পাসওয়ার্ড চলে যাবে। এই জন্য এটা প্রেরণকারীকে দ্বিধা করবেন না ও ঘাবড়াবেন না। এটা একটা চুড়ান্ত পর্যায়ের ফালতু চেষ্টা যা তাদের নিজেদেরই কিন্তু সাধারণ লোকেরা না বুঝার কারনে তাদের শিকার হয়।

পিসিতে টর দিয়ে ফেসবুক চালানো

যারা কম্পিউটারে টর ব্রাউজারের মাধ্যমে ফেসবুক চালান তাদের কম্পিউটারের আইপি বার বার পরিবর্তন হওয়ার কারনে অনেক সময় ফেসবুক কর্তৃক তাদের আইডিকে বন্ধ করে দেওয়া হয়। এই সমস্যা সমাধানের জন্য আমরা টর ব্রাউজারের সিটিংয়ে আমরা এমন কিছু কাজ করব যার ফলে টর ব্রাউজারে নির্দিষ্ট এক দেশের নাম শো করবে এবং সেই দেশেরই আইপি এড্রেস পরিবর্তন হতে থাকবে। এজন্য আপনাকে নিচের নির্দেশনা অনুযায়ী কাজ করতে হবে।

প্রথমে আপনি টর ব্রাউজারের ফোল্ডারে যান। এরপর ধারাবাহিক নিচে দেখানো ফোল্ডারগুলো খুলতে থাকুনঃ

Tor Browser\Browser\TorBrowser\Data\Tor

এরপর শেষ ফোল্ডারে একটি ফাইল পাবেন যার নাম torrc এই ফাইলকে কম্পিউটারের নোটপ্যাডের মাধ্যমে খুলে নিন। খোলে যাওয়ার পর সবার শেষে নিচের লেখাটি কপি পেষ্ট করুন।

ExitNodes {RO} StrictNodes 1

এরপর সেভ করে নেন। এবং টর ব্রাউজার রিস্টার্ট দেন। এখন আপনার টর ব্রাউজারের মাধ্যমে প্রত্যেক ওয়েব সাইটে শুধু রুমানিয়ান আইপি এড্রেস যাবে। মনে রাখবেন টর ব্রাউজারের মধ্যে প্রত্যেক ওয়েব সাইটের জন্য তিনটি করে প্রক্সি / নোডস আছে। আর এই সিটিংয়ের মাধ্যমে যা হবে তাহলো প্রত্যেক অয়েব সাইট যেমন ফেসবুক এবং অন্যান্য সাইটগুলোকে শুধু রুমানিয়ান কোন প্রক্সি শো করবে। যা রুমানিয়ার মধ্যেই একের পর এক পরিবর্তন হতে থাকবে। অর্থাৎ শেষ আইপি শুধু সেই দেশেই সিমাবদ্ধ থাকবে এবং টরের অন্য দুটি প্রক্সি অন্যান্য দেশেও শো করবে।

আপনি ইচ্ছা করলে রুমানিয়ার স্থানে অন্য দেশও দিতে পারেন। সে জন্য নিচের লেখার মধ্যে RO এর জায়গায় অন্য দেশের নামের সংক্ষিপ্ত রূপ বসালেই হবে।

ExitNodes {RO} StrictNodes 1

তবে দেশের নাম বসানোর ক্ষেত্রে শর্ত হলো ঐ দেশের নাম টর ব্রাউজারের লিস্টে থাকতে হবে। টরের সমস্ত কান্ট্রি কোড নেট সার্চ দিয়ে দেখে নিতে পারেন। অথবা এই লিংকেও পাবেন

http://www.b3rn3d.com/blog/2014/03/05/tor-country-codes/

টেলিগ্রামের ব্যপারে বিস্তারিত আলোচনা

টেলিগ্রাম চালানোর ব্যপারে সতর্কতা

গত অনেক দিন ধরেই টেলিগ্রামের ব্যাপারে অনেক ধরনের খবর প্রচারিত হচ্ছিল। যেহেতু মুজাহিদীন এবং তাদের সাথীরা এখন তা বেশি বেশি ব্যবহার করছেন তাই কাফের এবং

মুরতাদরাও সর্বোচ্চ চেষ্টা করছে তাদের মিডিয়াগুলোকে বন্ধ করে দেয়ার জন্য এবং তাদেরকে খোজ করার জন্য।

telegram এর প্রতিষ্ঠাতা Pavel Durov বলেছিল আমাকে আমরিকার নিরাপত্তা বাহিনী থেকে চাপ প্রয়োগ করেছে এবং আমাকে কিনে নেওয়ার চেষ্টা করা হয়েছিল। যাতে করে আমি তাদের জন্য এই টেলিগ্রাম software একটা ব্যাকডোর অর্থাৎ ফাদ তৈরি করে দেই যার মাধ্যমে তারা গোয়েন্দাগিরি করতে পারবে। কিন্তু আমি অস্বীকার করি এবং তেমনি ভাবে তাদের সব ধরনের চেষ্টা ও ইচ্ছাকে সে ফিরিয়ে দিয়েছে।

এবং পাভেল এটাও দাবি করেছে যে software গুলো আমেরিকা থেকে চলে না তার ওপর যদি তারা এত চাপ সৃষ্টি করতে পারে তাহলে যেটা আমেরিকা থেকে পরিচালিত হয় সেটাতে অবশ্যই তাদের শক্তির হস্তক্ষেপ থাকবে এবং সেগুলো american গোয়েন্দাদের মাধ্যমে পরিচালিত হবে। তার এই কথার ইশারা whatsapp এবং signal software এর দিকে ছিল কারণ এগুলো আমেরিকা থেকে প্রচার পরিচালিত হয়। এবং এগুলোতে পর্যাপ্ত পরিমাণ ফাঁদ তৈরি করা আছে।

সেই কথাগুলো তার নিজস্ব টুইটার একাউন্টে করেছে এবং এই কবরের বিস্তারিত আপনারা নিচের লিংকে পেয়ে যাবেনঃ

http://uk.businessinsider.com/telegram-founder-pavel-durov-claims-us-offered-backdoor-bribe-2017-6

এখানে এই কথা স্মরণ রাখতে হবে যে telegram কোম্পানি এবং তাদের নিরাপত্তা রাশিয়া থেকে পরিচালিত, যার ফলে আমেরিকান প্রভাব-প্রতিপত্তি তাদের উপর কম। তাই তারা অনেক চেষ্টার পরেও তাদের অধীনে আসে নি। কিন্তু তার পরেই রাশিয়ায় telegram কোম্পানির ওপর চাপ সৃষ্টি করে এবং দাবি করে যে যতক্ষণ না তোমরা ব্যবহারকারীদের তথ্য আমাদেরকে না দিবে ততক্ষন তোমাদেরকে রাশিয়া থেকে চলতে দেয়া হবে না। তখন টেলিগ্রাম company সরকারিভাবেই তাদের কোম্পানিকে রাশিয়ার মধ্যে রেজিস্ট্রি করায় যাতে করে এই ধরনের অধীনতা থেকে বাঁচতে পারে।

তবে এখানে একটি বিষয় খুব গুরুত্বের সাথে লক্ষ্য করা উচিত telegram কোম্পানির কাছে russia দাবি ছিল তারা ব্যবহারকারীদের তথ্য তাদের কে দেবে অন্যথায় তারা কোম্পানিকে

ব্লক করে দিবে। অতঃপর তারা শুধু কোম্পানিকে রেজেষ্টি করেই সমস্যাকে সমাধান করে ফেলে। এত সহজে তো রাশিয়া রাজি হওয়ার কথা নয়!!! সেই সময়ে অপর পক্ষ থেকে এই টেলিগ্রাম এর প্রতিষ্ঠাতা নিজে দাবি করে আসছে যে ব্যবহারকারীদের কোন ধরনের তথ্য দেওয়া হবে না এবং এটা নিয়ে কোনো ধরনের সমঝোতাও হবে না।

সাদার মধ্যে কিছু তো কাল থাকবেই। রাশিয়া যখন এত বড় দাবীর পরেও তাদেরকে তাদের দেশে জায়গা দিয়েছে তাহলে তো অবশ্যই সেখানে কোনো গোপন চুক্তি করেছে যাকে গোপন রাখা হয়েছে। বিস্তারিত খবর পড়ার জন্য নিচের লিংকে যানঃ

https://www.reuters.com/article/us-russia-telegram-security-idUSKBN19J1RK

অতঃপর ইন্দোনেশিয়ার টেলিগ্রাম সফটওয়্যার কে ব্লক করার হুমকি দিয়েছে এবং তার ব্যবহারকে সীমাবদ্ধ করে দেয়। যার পরিপ্রেক্ষিতে টেলিগ্রাম এর প্রতিস্টাতা ঘোষণা দেয় যে তারা আলাদা একটি গ্রুপ তৈরি করেছে যারা সন্ত্রাসী মানে মুজাহিদের চ্যানেলগুলোকে খুজবে এবং সেগুলো telegram থেকে ডিলিট করে দিবে। তাদের প্রকাশনাগুলোকে বন্ধ করে দিবে। অর্থাৎ তার উদ্দেশ্য হচ্ছে তাদের সবকিছুকে আটকে দেয়া। এবং তার দাবি ছিল যে এক মাসের মধ্যে হাজারের উপর চেনেল তারা বন্ধ করে দিয়েছে এবং এই সিস্টেমটাকে তারা আরও উন্নত করেছে। এই খবরটা পরিপূর্ণ পড়ার জন্য নিচের লিংক থেকে যানঃ

http://www.aljazeera.com/news/2017/07/telegram-blocks-terror-content-indonesia-threat-170716041113324.html

পুরা কথার সারসংক্ষেপ করছে telegram company অনেক চাপের মধ্যে আছে এবং তারা মুজাহিদীনদের চ্যানেলগুলোকে দেরি করা ছাড়াই বন্ধ করে দিচ্ছে। কিন্তু তারপরও সবচেয়ে বড় ভয়ের বিষয় হচ্ছে তারা ব্যবহারকারীদের মেসেজ এবং অন্যান্য তথ্য কাউকে দিয়ে দিচ্ছে না তো ?!!! এই জন্য নিরাপত্তা দাবি এটাই হবে যে টেলিগ্রামের মাধ্যমে কোন ধরনের ব্যক্তিগত যোগাযোগ করা যাবে না বিশেষ প্রয়োজনে অন্য কোন লিঙ্কের মাধ্যমে নিরাপত্তা সাথে দিতে হবে।

টেলিগ্রামকে টরের সাথে কানেক্ট

প্রথমে টর ব্রাউজার খোলবেন এবং খুলা অবস্থায় রেখে দিবেন। কেননা টেলিগ্রাম মেসেঞ্জার সেটার সাথে কানেক্ট হবে। যতক্ষণ টর ব্রাউজার খোলা না হবে ততক্ষণ টেলিগ্রাম নেট

কানেক্ট হবে না। টর ব্রাউজার খোলার পর টেলিগ্রাম খোলবেন। টেলিগ্রাম সিটিংসের মধ্যে যাবে। সেখানে Connection type এর মধ্যে যাবে। এরপর TCP with custom socks5-proxy এই আপশনটা সিলেক্ট করবে। তার মধ্যেঃ

Hostname: localhost
port: 9150

এটা লিখবে। তারপর সেভ করে দ্বিতীয়বার টেলিগ্রাম চালু করবে। এখন টেলিগ্রাম টর ব্রাউজারের সাথে চলবে।কিন্তু এর জন্য টর ব্রাউজার চালু করা জরুরি।

এখন বাস্তবেই টেলিগ্রাম টরের সাথে চলছে এটা দেখার জন্য সিটিংসের মধ্যে show all sessions কে দেখে নিবে।সেখানে আপনার আইপি এড্রেস ও দেশের নাম দেয়া আছে, যা পরিবর্তন হয়ে গেছে।

আর এভাবে টেলিগ্রামকে টরের সাথে কানেক্ট করার ফায়েদা হচ্ছে সাধারণ নেটওয়ার্কের সাথে চলবেনা। অর্থাৎ ইন্টারনেট কানেকশন ড্রপ হওয়ার অবস্থায় আইপি এড্রেস হ্যাঁক হওয়ার কোন আশংকা নাই।কেননা এখন আপনার টেলিগ্রাম টর ছাড়া একেবারেই চলবেনা। এভাবেই ভিপিএন ছাড়া টরের মাধ্যমেও টেলেগ্রাম চালানো যায়।

প্রক্সি সেটিংয়ের দ্বিতীয় নিয়ম

নিচের দুইটা লিংকে ক্লিক করার পর একটা বক্স আসবে। সেখানে ENABLE ক্লিক করবেন। অত:পর কম্পিউটারে Tor browser ও মোবাইলে Orbot চালু করে আবার টেলিগ্রামে প্রবেশ করবেন।

মোবাইলের জন্য:

https://t.me/socks?server=127.0.0.1&port=9050

কম্পিউটারের জন্য:

https://t.me/socks?server=localhost&port=9150

বি:দ্র: যদি লিংকে চাপ দেয়ার পর শুধু কানেক্টিং দেখায় ও নতুন কোন মেসেজ বা পোষ্ট না আসে তাহলে বুঝবেন আপনার Tor বা Orbot চালু নেই।

আপনি বিভিন্ন দেশের আইপির মাধ্যমেও প্রক্সি সেটিং করতে পারেন। এর মধ্যে সবচেয়ে নিরাপদ হচ্ছে Socks5 proxy গুলো। নিচের লিংকে এগুলোর বিশাল ভান্ডার পাবেন যেখানে মুহুর্তে মুহুর্তে নতুন প্রক্সি দেয় যা শুধু ক্লিক করার মাধ্যমেই একটিভ করতে পারেন।

https://t.me/TgProxies

টেলিগ্রাম আইডি নষ্ট হওয়া থেকে রক্ষার উপায়

টেলেগ্রাম নিরাপত্তা জনিত সার্থেই আইডি লগিনের পদ্ধতি একটু কঠিন করে রেখেছে। যার ফলে অন্যগুলোর মত পাসওয়ার্ড দিয়ে পুনরায় লগিন করা যায় না। বরং নাম্বার চালু রাখতে হয় অথবা আইডি অন্য কোন ডিভাইসে লগিন করে রাখতে হয়। যাতে আবার আপনার মোবাইলে লগিন করার সময় কোড মেসেজ দেখতে পারেন।

কিন্তু অধিকাংশ সময় textnow এর নাম্বার চালু থাকে না এবং আইডি অন্য কারো মোবাইলে বা পিসিতে লগিন করে রাখার সুযোগ থাকে না। ফলে কোন কারণে সফটওয়্যারে ঝামেলা হলে আইডি ফিরত পাওয়া যায় না।

আমরা আজ সহজ ও পরিক্ষিত একটি সমাধান নিয়ে আলোচনা , যার ফলে আপনাদের আইডি রক্ষা করতে পারবেন ইংশাআল্লাহ। বিষেশ করে সফরে আমানিয়্যাতের জন্যে সফটওয়্যার কেটে দিলেই আইডি হাড়ানোর ঝামেলা নেই ইনশাআল্লাহ।

প্রথমে টেলিগ্রাম আইডিকে sd card এর মধ্যে মুভ করে নেন। এবং মেমোরিটি মোবাইল থেকে খুলে নিন। এতে করে টেলি এপ্সটি মোবাইলে দেখাবে না। যদি শো করে তাহলে মোবাইল থেকে টেলি এপ্সকে আনইন্সটল করে ফেলুন। এরপর প্রয়োজনের সময় অথবা নিরাপদ স্থানে যাওয়ার পরে শান্তমনে মেমোরিটি সেটে প্রবেশ করানোর সাথে সাথেই টেলি এপ্সটি আগের আইডি সহ চলে আসবে ইনশাআল্লাহ। যদি না আসে, তাহলে টেলিগ্রাম এপ্সকে ইন্সটল করুন। ওকে হয়ে যাবে ইনশাআল্লাহ।

sd card এ মুভ করার পদ্ধতি

সব মোবাইলেই মুভ করার সিস্টেম থাকে। তবে ভিন্ন ভিন্ন পদ্ধতিতে। তাই ভালভাবে খোজে নিতে হবে। সাধারনত নিচের দুইটা পদ্ধতিই থাকেঃ-

১/settings→ applications→ application managar

2/settings→ apps

এখন আপনার সামনে আপনার মোবাইলে থাকা সবগুলো এপ্স উপস্থিত হবে। এখন টেলেগ্রামে ক্লিক করুন। তারপর move to sd card এ ক্লিক করে Moving লেখাটা চলে যাওয়া পর্যন্ত অপেক্ষা করুন। এর পরেও সফর ভাবে মুভ হয়ে যাবে ইনশাআল্লাহ।

peer-to-peer বন্ধ করার নিয়ম

আমরা জানি টেলিগ্রামে কলের মাধ্যমে অন্যদের সাথে যোগযোগ করা যায়। এখানে কলের জন্যে দুই ধরনের Relay ব্যবহার করা হয়। একটি হচ্ছে টেলেগ্রামের প্রক্সি ব্যবহার করা, এখানে কল ইঙ্ক্রিপ্টেড হওয়ার কারণে ভয়েস একটু দুর্বল হয়ে থাকে। অন্যটা হচ্ছে peer-to-peer কল করা। এখানে ভয়েসের কোয়ালিটি ভাল হয়ে থাকে। কিন্তু এটা জন্যে অপর সাইডের ব্যক্তির সাথে আপনার নিজস্ব IP ব্যবহার করে যোগাযোগ করা হয়।

ভয়ের ব্যপার হচ্ছে সিস্টেমগত ভাবেই প্রত্যেকটা টেলিগ্রাম আইডিতে কলের অপশন চালু করা থাকে। সেই সাথে peer-to-peer চালু থাকে। এর ফলে অনাকাঙ্ক্ষিত কেহ যদি আপনাকে কল করে আর আপনার প্রক্সি চালু না থাকে তাহলে সরাসরি আপনার IP দিয়ে কল আসবে। আর এই কলের ডিটেইলস বের করতে পারলেই সে আপনার অবস্থান পেয়ে যাবে।

সমাধানঃ টেলিগ্রামে সেটিং থেকে peer-to-peer বন্ধ করে দিন। এর নিয়ম হচ্ছেঃ

Settings থেকে Privacy and Security যাবেন। সেখানে একেবারে নিচে Peer-to-peer অপশনে ক্লিক করে Nobody ক্লিক করবেন।

বিঃদ্রঃ অবশ্যই প্রক্সি চালু করে রাখবেন। কারণ আপনার IP অন্য কেহ না পেলেও টেলেগ্রাম কম্পানী কিন্তু পেয়ে যাচ্ছে।

টেলিগ্রামে কলের অপশন বন্ধ

টেলিগ্রামে কলের অপশন বন্ধ রাখা একটি আবশ্যকীয় কাজ। কারণ এর মাধ্যমে আপনার আইপি হ্যাক হওয়ার সম্ভাবনা থাকে।

নিয়ম: Setting > Privacy and Security > Calls অপশনে nobody টিক দিয়ে দিবেন।

এন্টিভাইরাস বুট

টেলিগ্রামের এন্টিভাইরাস বুটের মাধ্যমে যে কোন লিংক ও ২০ এমবির কম যেকোন ফাইল ভাইরাস স্ক্যান করতে পারবেন। তার জন্যে প্রথমে @DrWebBot ঢুকুন। পরে /start ক্লিক করুন। এর পর /setting ক্লিক করুন। সেখানে Notifications > Relpy on every link or file ক্লিক করুন। পরে এক্সিট ক্লিক করে বের হোন। পরে আপনি কোন লিংক কপি করে এখানে পেষ্ট অথবা কোন ফাইল এখানে আপলোড করলে দেখাবে ভাইরাস আছে কিনা। জাযাকাল্লাহ।

টেলিগ্রামে স্ক্রীনশট

অনেকে টেলিগ্রামে স্ক্রীনশট নিতে পারেন না। এটা মূলত হয়ে থাকে যাদের টেলিগ্রামে পাসকোড চালু করে থাকেন, যাতে করে বের হওয়ার পর লক হয়ে যায়। সেখানে প্রথম থেকেই নিরাপত্তার জন্যে স্ক্রীনশট নেয়ার অপশন বন্ধ করা থাকে যাতে এখানে তথ্য কোথাও শেয়ার না করা যায়।

সমাধান: Setting থেকে Privacy and Security যাবেন। সেখানে Passcode Lock অপশনে গিয়ে নিচে দেখবেন Allow Screen Capture অপশনটা চালু করে বের হয়ে আবার ঢুকুন। স্ক্রীনশট নিতে পারবেন ইনশাআল্লাহ।

এড অপশন বন্ধ

কিছু আইডি নিজেদের খারাপ স্বার্থের জন্যে অন্যদের আইডিকে তাদের গ্রুপে অনিচ্ছাকৃত জয়েন কর দেয়। যা ভিবিন্ন ধরনের নিরাপত্তা ঘাটতি সহ অনেক ঝামেলা সৃষ্টি করছে। এই সমস্যা সমাধানের জন্যে সেটিং থেকে চ্যানেল বা গ্রুপে এড করার অপশন বন্ধ করে দিতে হবে, যাতে কেহ আপনাকে অনিচ্ছাকৃত যোগ না করতে পারে।

মোবাইলে জন্যঃ Settings থেকে Privacy and Security অপশনে যাবেন। সেখানে Privacy মেনুতে Groups এ ক্লিক করে MY Contacts এ টিক দিয়ে দিবেন।

পিসির জন্যঃ Settings থেকে Privacy and Security মেনুতে গিয়ে Group invite settings এ ক্লিক করে MY Contacts এ টিক দিয়ে দিবেন।

টেলিগ্রাম একাউন্ট ডিএক্টিভ

টেলেগ্রাম একাউন্ট ডিলিটের কাজটি দুইটা স্টেপে করুন:

১/ প্রথমে টেলেগ্রামের ডিলিট পেইজে যান।

https://my.telegram.org/auth?to=deactivate

২/ নাম্বার প্রবেশ করানোর পর টেলেগ্রামের আইডিতে ডিলিট কোড আসবে। সেটাকে কপি করে ডিলিট পেইজে পেস্ট করুন।

একাউন্ট ডিএক্টিভ করার পর সমস্ত আইডি, চ্যানেল ও গ্রুপ কেটে যাবে। এবং এই আইডিতে আর ফিরে আসা যাবে না। এই নাম্বারে আবার নতুন করে আইডি করতে হবে ফিরে আসার জন্য।

webTRC থেকে বাঁচুন

যেমনটা সর্বদা বলা হয়ে থাকে পূর্ন নিরাপত্তা কখনোই একটা ডিভাইস বা সফটওয়ারের মাধ্যমে হয় না। বরং এর জন্যে অনেক পরিমানের সতর্কতা গ্রহন করা আবশ্যক। সামনে আলোচনাটা অনেক গুরুত্বপূর্ন, কারণ অনেকেই হয়ত VPN ব্যবহার করেন বা সামনে করা ইচ্ছা আছে। তা সত্যেও webTRC আপনার আসল আইপি প্রকাশ করে দেয় যত শক্তিশালী VPN ব্যবহার করা হোক না কেন।

WEB RTC : এটা হচ্ছে নতুন একটি ইন্টারনেট প্রোটোকল যা জাভা স্ক্রিপ্টের মাধ্যমে তৈরি হয়েছে। এবং এটা আপনার আসল IP প্রকাশ করে দিবে VPN ব্যবহারের পরেও।

ব্রাউজারের মধ্যে NO Script প্লাগিন সংযুক্ত করার ফলে java থেকে মুক্তি পাওয়া গেলেও মাঝে মাঝে বন্ধ হয়ে যাওয়ার ভয় থাকে। তাই সেটিং থেকে বন্ধ করে নেয়াটাই উত্তম।

ব্রাউজার থেকে webTRC বন্ধ করার নিয়মঃ

অনলাইনে দেখুনঃ

https://pastethis.at/webTRCbn

PDF ডাউনলোড করুনঃ

https://archive.org/download/WEBRTC/WEB%20RTC.pdf

ওয়েব সিকিউরিটি সার্টিফিকেট

যেকোন ওয়েব সাইট ঢুকেন, আপনি হয়তো http অথবা https ব্যবহার করছেন। এই দুইয়ের মাঝে শুধু সিকিউরিটি সার্টিফিকেটের পার্থক্য। সিকিউরিটি সার্টিফিকেট এর অর্থ হচ্ছে তাদের সাথে আপনার কানেকশন নিরাপদ অর্থাৎ যেই ইউজার নেম ও পার্সওয়াড ব্যবহার করবেন তা গোপন থাকবে। মধ্যবর্তি ইন্টারনেট প্রোভাইডার এগুলো ট্রেস করতে পারে না। তাই বিশেষ ভাবে খেয়াল রাখবেন, আপনি যে ওয়েবসাইটে ইউজার নেম ও পার্সওয়ার্ড ব্যবহার করছেন সেটা নিরাপদ কিনা? এটার দেখার পদ্বতিটি হচ্ছে, আপনি যে কোন ব্রাউযারে ওয়েবসাইট খুলে লিংক ঘরের একেবারে বামে ক্লিক করবেন, যেটা ছবিতে দেখানো হয়েছে। তখন সেখানে দেখতে পাবেন কানেকশন নিরাপদ কি না। আর যে সমস্ত সাইট এটা চায় না তাদের কানেকশন সিকিউর হয় না, আর এই ক্ষেত্রে প্রয়োজন ও হয় না। যেমন দ্বিতীয় ছবিতে বিবিসি উর্দু ওয়েবসাইট যাতে সিকিউর নয়। এবং সিকিউরিটি চাওয়াও হয় না।

নোটঃ অধিকাংশ ফিশিং সাইট সিকিউরিটি কানেকশন ঠিক থাকে না। তাই খেয়াল রাখবেন ফেইসবুক বা টুইটার ইত্যাদি যখন কোথাও ওপেন করবেন তখন অবশ্যই দেখে নিবেন কানেকশন নিরাপদ কিনা । অনেক সময় ফিশিং সাইটের লিংক এমন ভাবে বানানো হয় যে বুঝাই যায় না যে সেটা নকল। তাই এই পদ্ধতিতে চেক করে নিবেন।

Advanced System Care Ultimate

কম্পিউটার ব্যবহারকারীদের জন্য ভাল একটি নিরাপত্তা সফটওয়্যার। এই সফটওয়্যার আপনার পিসির স্পীডও বাড়িয়ে দিবে. অন্যান্য এন্টি ভাইরাসের মতো আপনার পিসির স্পীড কমিয়ে দিবেনা বরং যথেষ্ট পরিমান বাড়িয়ে দিবে ইনশাআল্লাহ।

এই সফট ওয়্যারের মধ্যে নিরাপত্তা সম্পর্কিত কিছু বৈশিষ্ট আছে। এবং তার নিজিস্ব এন্টি ভাইরাসও আছে। মোটকথা এই সফটওয়্যার পৃথক কিছু বৈশিষ্ট রাখার পাশাপাশি এটি একটি পূর্ণ নিরাপত্তা সফটওয়্যার। এই সফটওয়্যার ৩০ দিনের ট্রায়াল দেয়। তবে আমরা এখানে ক্র্যাক করার পদ্ধতি বলে দিব যার মাধ্যমে আপনি এটাকে ফ্রী ব্যবহার করতে পারবেন।

সফটওয়্যারটিকে তার অফিসিয়াল সাইট থেকে ডাউনলোড করুনঃ

http://www.iobit.com/en/advanced-systemcare-antivirus.php

এখান থেকে তার ফ্রী ভার্সন ডাউনলোড করুন। নিচে প্রদত্ত লিংকের থেকে তার ক্র্যাক ফাইল ডাউনলোড করুন

https://my.pcloud.com/publink/show?code=XZmKl47Z9CPNVgAqc3fPkHlnQbMaQzdOb37X

এখন সফটওয়্যার ইনষ্টল করুন। এরপর ক্র্যাক করুন। দুইটি ক্র্যাক ফাইল আছে এখানে। ক্র্যাক করার পদ্ধতি আপনি ফোল্ডারের মধ্যে দেখতে পারেন। প্রথম ক্র্যাক যদি কাজ না করে তাহলে দ্বিতীয় ক্র্যাক চালাবেন। যখন ক্র্যাক হয়ে যাবে তখন তাকে আপডেট করে নিবেন। স্ক্রিনে যে ফক্স লেখা আসে আপনি তাতে ক্লিক করুন।
ক্র্যাক করার পরেই একটা স্ক্রিন চালু হবে। আর যদি না খোলে তাহলে quick settings এর মধ্যে পাবেন। এখন দেখে নিন কি কি ফিচার আপনি চালাতে ইচ্ছুক।
নোটঃ Browser Anti-Tracking এই বিষয়টি যদি লিষ্টে অন করা থাকে তাহলে প্রত্যেকবার ব্রাউজার বন্ধ হওয়ার পর হিষ্ট্রি ডিলিট করে দিবে। তবে কুকিজ ডিলিট করবেনা শুধু হিষ্ট্রিই কেটে দিবে।
এর মধ্যে একটি অপশন আছে Secure File Deletion এর মাধ্যমে আপনি যে ফাইল ডিলিট করবেন তা স্থায়ী ভাবে ডিলিট হয়ে যাবে। এবং কোন রিকভার সফটওয়্যারের মাধ্যমে ফিরে

আসবেনা। তবে এভাবে ডিলিট করতে কিছুটা সময় নিবে। আপনি যদি এভাবে ডিলিট করতে চান তাহলে এই অপশন অবশ্যই চালু করবেন।
এখন আপনি ঐ স্ক্রীন বন্ধ করে দিন। মেইন স্ক্রীনে মেনু বারে Antivirus মেনু ও Speed up মেনু আসবে। আর সেখানেই Clean & Optimize অপশনে যাবেন এবং সেখানে গিয়ে সিলেক্ট অল করুন।

এরপর আপনি Toolbox মেনুতে যাবেনঃ-
সেখানে সব ফিচার ডাউনলোড করা লাগবে। তবে সেটা এই সফটওয়্যারের ভেতরেই থাকবে পৃথক ভাবে ডাউনলোড এবং ইনস্টল করতে হবেনা। শুধু Obit Products ছাড়া। এটাকে পৃথক ভাবে ডাউনলোড ইনস্টল করতে হবে। এখন আপনি দেখে নিন কোন কোন ফিচার আপনার কাজে আসবে আপনি সেগুলো ডাউনলোড করে নিন।
File Shredder অনেক কাজের জিনিস। অর্থাৎ যেটাকে আপনার হার্ডিস্ক থেকে একবার ডিলিট করা হয়েছে সেটাকে স্থায়ী ভাবে ডিলিট করে দিবে। যাতে করে কোন নাম নিশানা বাকি থাকবেনা। আপনি যদি কোন গোপন ফাইল ডিলিট করতে ইচ্ছা করে এমন ভাবে যাতে হার্ডিস্কে এর কোন নাম নিশানা বাকি না থাকুক এবং রিকভার না হোক তাহলে অবশ্যই এটাকে ব্যবহার করবেন।
Undelete ফিচারটা হলো আপনার কোন ফাইল ডিলিট হয়ে গেল এখন আপনি এটাকে রিকভার করতে চাচ্ছেন তখন একটা পর্যায় পর্যন্ত আপনি রিকভার করতে পারবেন।

বাকি ফিচারগুলো আপনি নিজেই দেখে নিন। ইনস্টল হওয়ার পর ডেস্কটপের উপরে আপনি একটা অপশন দেখতে পাবেন। এর মধ্যে ব্রাশ ওয়ালা অপশনে ক্লিক করে আপনি রেম খালি করতে পারবেন যা যথেষ্ট পরিমান রেম খালি করে দিবে। এবং আপনার কম্পিউটার অনেক দ্রুত কাজ করবে।

উইন্ডোজ টেনে অটো আপডেট বন্ধ

উইন্ডোজ ১০ এ নিশ্চয়ই খেয়াল করেছেন, এই অপারেটিং সিস্টেমটি নিজ থেকেই সফটওয়্যার আপডেট ডাউনলোড করে নেয়। অনেক সময় এ কারণে অত্যাধিক পরিমাণ ইন্টারনেট ডেটা খরচ হয়ে যায়। যাদের ইন্টারনেট ডেটা সীমিত তাদের জন্য এটা বেশ দুশ্চিন্তার কারণ।
উইন্ডোজ ১০ এর সেটিংস থেকে অটোম্যাটিক আপডেট বন্ধ করার সরাসরি কোনো অপশন

নেই। কিন্তু একটু কৌশল খাটিয়ে আপনি সহজেই উইন্ডোজ ১০ এর অটো আপডেট বন্ধ করে রাখতে পারেন।

১ম পদ্ধতিঃ ইন্টারনেট নেটওয়ার্ক 'মিটারড কানেকশন' হিসেবে সেট করা

যারা ওয়াইফাই হটস্পটে ইন্টারনেট ব্যবহার করেন, তারা যদি ইন্টারনেট কানেকশনটি 'মিটারড' হিসেবে সেট করে রাখেন, তাহলে উইন্ডোজ আপডেট ডাউনলোড হবেনা। তবে কানেকশনের নাম/হটস্পট ডিভাইস পরিবর্তিত হয়ে পুনরায় অটো আপডেট চালু হয়ে যাবে। সুতরাং কানেকশনের নাম বা হটস্পট ডিভাইস পরিবর্তন করলে সেটি নতুনভাবে 'মিটারড' হিসেবে সেট করতে হবে। কোনো ওয়াইফাই কানেকশনকে 'মিটারড' হিসেবে চিহ্নিত করার উপায় এখানে দেয়া হলঃ-
পিসি আপনার ওয়াইফাই হটস্পটের ইন্টারনেটে সংযুক্ত থাকা অবস্থায় স্টার্ট বাটনে ক্লিক করে স্টার্ট মেন্যু থেকে 'settings' ওপেন করুন। সেটিংস থেকে 'Network and Internet' সেকশন ওপেন করুন
সেখানে 'Wifi' সেকশনে গিয়ে ডানদিকে আসা 'Advanced Options' এ ক্লিক করুন এখন যে পেজটি আসবে সেখানে 'মিটারড কানেকশন' শিরোনামের নিচে 'সেট অ্যাজ মিটারড কানেকশন' লেখা সুইচে ক্লিক করে সেটি 'অন' করে দিন। ব্যাস, এখন থেকে আর আপনার বর্তমান ওয়াইফাই ইন্টারনেট সংযোগে উইন্ডোজ ১০ এর আপডেট স্বয়ংক্রিয়ভাবে ডাউনলোড হবেনা।

২য় পদ্ধতি: উইন্ডোজ আপডেট সার্ভিস' বন্ধ করে রাখাঃ-

কিবোর্ডের উইন্ডোজ বাটন চাপ দিয়ে ধরে রেখে R বাটন চাপ দিয়ে রান কমান্ড চালু করুন (অর্থাৎ Windows + R প্রেস করুন)। এবার যে রান কমান্ড বক্স আসবে, সেই বক্সের মধ্যে services.msc লিখে এন্টার বাটনে চাপ দিন
এখন একটি উইন্ডো ওপেন হবে, যেখানে লিস্ট আকারে অনেকগুলো সার্ভিসের নাম লেখা থাকবে। এর মধ্য থেকে লিস্টের শেষদিকে 'Windows Update' সার্ভিস খুঁজে বের করে সেটির উপর ডাবল ক্লিক দিয়ে সার্ভিসটির প্রোপার্টিজ মেন্যু ওপেন করুন।
এখানে 'জেনারেল' ট্যাবে 'Startup Type' এর জন্য 'Disabled' অপশন বাছাই করে 'OK' বাটনে ক্লিক করুন। এখন কম্পিউটার রিস্টার্ট নিতে চাইবে। রিস্টার্ট দিন।

FireFox ব্রাউজারে নিরাপত্তা

মোবাইল এবং পিসিতে সাধারন ব্রাউজারের মধ্যে সবচেয়ে ভাল হচ্ছে FireFox. যখন VPN ব্যবহার করা হয় তখন এটা দিয়েই সরাসরি জিহাদী সাইটে প্রবেশ সহ সব কাজই করা যায়। তবে এখানে সেটিং থেকে কিছু সিস্টেম ঠিক করে নেওয়া জরুরী। আমরা আজ সেগুলো নিয়ে আলোচনা করব।

প্রথমে Firefox খুলুন এবং সার্চ বক্সে লিখুন about:config ও ক্লিক করুন। এরপর I'll be careful, I promise ক্লিক করুন।

এখন আপনার সামনে বিশাল চার্ট খুলে যাবে সেখানে সার্চ বক্সে নিচের লেখাগুলো লিখে সার্চ দিয়ে ভ্যালুগুলো ঠিক করে নিন।

১/ সার্চ করুন privacy.trackingprotection.enabled এটার ভ্যালু করুন True
>> এটার মাধ্যমে আপনি ট্রেকিং থেকে রক্ষা পাবেন।
২/ সার্চ করুন geo.enabled এটার ভ্যালু করুন False
>> এটা ব্রাউজারে লোকেশন ট্রেস করা থেকে রক্ষার জন্য।
৩/ সার্চ করুন browser.safebrowsing.enabled এটার ভ্যালু করুন False
>> এটা গোগলকে ব্রাউজার প্রটেকশন থেকে বাধা দেয়ার জন্য কারণ তারা ব্যবহারকারীর তথ্য জমা করে।
৪/ সার্চ করুন browser.safebrowsing.malware.enabled এটার ভ্যালু করুন False
>> এটা গোগলকে ব্রাউজার প্রটেকশন থেকে বাধা দেয়ার জন্য কারণ তারা ব্যবহারকারীর তথ্য জমা করে।
৫/ সার্চ করুন dom.event.clipboardevents.enabled এটার ভ্যালু করুন False
>> এটা সাইটগুলোকে আপনার কপিকৃত জিনিস জানা থেকে বাধা দেয়।
৬/ সার্চ করুন network.cookie.cookieBehavior এটার ভ্যালু করুন ১
>> এটা ভিবিন্ন সাইট থেকে কুকিস সংগ্রহ করা থেকে রক্ষা করে। এবং থার্ড পার্টি টুলস সমূহকে কুকিস নেয়া থেকে বাধা দেয়।
৭/ সার্চ করুন network.cookie.lifetimePolicy এটার ভ্যালু করুন ২
>> এটা কোন সাইট থেকে বের হওয়ার সাথে সাথে কুকিজ মুছে দেয়।
৮/ সার্চ করুন browser.cache.offline.enable এটার ভ্যালু করুন False

>> ডিভাইসে Cache সংগ্রহ করা থেকে বাধা দেয়।

৯/ সার্চ করুন browser.send_pings এটার ভ্যালু করুন False

>> এটা আপনি কোন কোন সাইট ব্রাউজ করছেন ও মাউসে ক্লিক করছেন তা কেহ জানা থেকে রক্ষা করে।

১০/ সার্চ করুন webgl.disabled এটার ভ্যালু করুন True

>> এটা আপনাকে webgl থেকে রক্ষা করবে।

১১/ সার্চ করুন dom.battery.enabled এটার ভ্যালু করুন False

>> এটা আপনার ডিভাইসের ব্যাটারির চার্যের মাধ্যমে অবস্থান জানা থেকে রক্ষা করবে।

১২/ সার্চ করুন browser.sessionstore.max_tabs_undo এটার ভ্যালু করুন ০

>> ভিবিন্ন সাইটে লগিন আইডি সেইভ রাখা থেকে বাঁচায়।

WEB RTC থেকে মুক্তির জন্যে নিচের কাজগুলো করুনঃ

> সার্চ করুন media.peerconnection.enabled এটার ভ্যালু করুন False

> সার্চ করুন media.peerconnection.turn.disable এটার ভ্যালু করুন True

> সার্চ করুন media.peerconnection.use_document_iceservers এটার ভ্যালু করুন False

> সার্চ করুন media.peerconnection.video.enabled এটার ভ্যালু করুন False

> সার্চ করুন media.peerconnection.identity.timeout এটার ভ্যালু করুন ১

বিঃদ্রঃ মোবাইল এবং পিসিতে সিস্টেম একই রকম।

অনলাইনে পড়ুনঃ

https://pastethis.at/FireFoxBN

PDF ডাউনলোড করুনঃ

https://archive.org/download/FireFoxBN/FireFox.pdf

লিনাক্স কম্পিউটার হ্যাকঃ পদ্ধতি ও সমাধান

লিনাক্স ব্যবহারকারীদের জন্য সতর্কবার্তা। লিনাক্সে এমন বাগ পাওয়া গেছে যা কম্পিউটারকে হ্যাক করতে পারে ও পাসওয়ার্ড ভেঙ্গে ফেলতে সক্ষম।

যে কম্পিউটার লিনাক্সের ডিস্ট্রিবিউশন থেকে কাজ করে সেটাকে সহজেই হ্যাক করা সম্ভব হয়েছে এবং সে কম্পিউটার সাইনিং করার জন্য পাসওয়ার্ড ভুল দিয়ে সাভাবিকভাবে ঢুকা যাচ্ছে!!! এর ধারাবাহিকভাবে কী বোর্ডের BackSpace বাটনে ২৮ বার ক্লিক করলেই যথেষ্ট। এটা কীভাবে সম্ভব !?

এই দুর্বলতা Valencia ইউনিভার্সিটির দুজন নিরাপত্তা-গবেষক প্রকাশ করেছে। কেননা তারা একাধিক কম্পিউটারকে হ্যাক করতে সক্ষম হয়েছে যা লিনাক্স সিস্টেমের বিভান্ন ডিস্ট্রিবিউশন ব্যবহার করে। এবং সিস্টেমকে বুট করার জন্য BackSpace বাটনে ধারাবাহিক ২৮ বার চাপ দেয়ার পরে পাসওয়ার্ড ছাড়াই প্রবেশ করতে সক্ষম হয়েছে।

সিস্টেমের নিউক্লিয়াসে অথবা স্বয়ং সিস্টেমে দুর্বলতা দেখা যাচ্ছে না।বরং বাগ পাওয়া ভিন্ন আরেক জায়গায় যা Grub2 বা স্টান্ডার্ড বুট লোডার Grand Unified Bootloader নামে পরিচিত। যাকে লিনাক্সের অধিকাংশ ডিস্ট্রিবিউশন ইউজ করে থাকে কম্পিউটারকে চালু করার সময় বুট করার জন্য।

দুর্বলতাটি 1.98 (ডিসেম্বর২০০৯) থেকে 2.02 পর্যন্ত মুক্ত হওয়া সকল ভার্সনেই সফলভাবে পাওয়া গেছে। আর এটার জন্যে BackSpace বাটনে ২৮ বার ধারাবাহিক চাপ দিতে হয় Grub rescue shall খুলা পর্যন্ত। ফলে rescue shall কম্পিউটারের অরক্ষিত এক্সেসের অনুমতি দেয়। তখন হ্যাকার ডিভাইসে সংরক্ষিত তথ্যাদি নিয়ন্ত্রণ, মুছে ফেলা, চুরি করা বা ডিভাইসে ক্ষতিকর সফটওয়্যার ইন্সটল করতে পারে।

সে দুর্বলতাকে Grub2 বলা হয়ে থাকে। আর এটা ২০০৯ সন থেকে আজ পর্যন্ত লিনাক্স ডিস্ট্রিবিউশনের পুরাতন অনেক ভার্সনে আক্রমণ করেছে। দুজন গবেষক দুর্বলতার নিরাপত্তা সমস্যা সমাধানের জন্যে Patch তৈরি করেছে। যা নিচের লিংক থেকে ডাউনলোড করুনঃ

http://hmarco.org/bugs/patches/0001-Fix-CVE-2015-8370-Grub2-user-pass-vulnerability.patch

নিজের ডিভাইসে পাসওয়ার্ড ভাঙ্গার অভিজ্ঞতা অর্জন করুন। আপনি যদি Ubuntu বা Debian ডিস্ট্রিবিউশন ব্যবহারকারী হয়ে থাকেন তাহলে নিরাপত্তা আপডেট হিসাবে Patch এর মাধ্যমে সেই বাগকে সংশোধন করে ফেলুন যা বাটন চাপার মাধ্যমে। এগুলোর প্যাচ নিচে দেয়া হল।

Ubuntu - https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003218.html

Debian - https://security-tracker.debian.org/tracker/CVE-2015-8370

প্রযুক্তি বিষয়ক প্রশ্ন-উত্তর

প্রশ্নঃ আপনি কি নিরাপদে ফেসবুক এবং Google সক্রিয় করতে সিম নম্বরগুলি ব্যবহার করতে পারেন?

জবাবঃ বেশীরভাগ SIM গুলো ব্যবহারকারীর ব্যক্তিগত তথ্যের মাধ্যমে নিবন্ধিত করা হয়। যদি আপনি যে সিম কার্ডটি ব্যবহার করেন তা অন্য কারো তথ্যের মাধ্যমে নিবন্ধিত হয় বা ব্যক্তিগত তথ্যের মাধ্যমে নিবন্ধিত নাও হয় তারপরেও প্রথম SMS টি পাওয়ার সাথে সাথেই আপনার অবস্থান সনাক্ত হয়ে যায়। প্রত্যেকবার মোবাইলের সাথে সিম সংযোগের সময় ফোন অপারেটর কোম্পানিগুলো সিমের নাম্বার এবং আপনার ফোনের IMEI ক্রমিক নম্বরটি সংরক্ষণ করে। তাই ভুল নিরাপত্তা গ্রহণে বিশেষ ভাবে উল্লেখযোগ্য যাতে অনেক ব্যবহারকারী পতিত হয়, অনেকে নিজস্ব তথ্য দিয়ে রেজিস্টার করা ছাড়া সিম সংগ্রহ করে যোগাযোগের জন্যে এবং কিছু দিন পরপর একটা করে সিম পরিবর্তন করে থাকে। কিন্তু অপারেট ঠিকই জেনে যায় যে দ্বিতীয় সিম ব্যবহারকারীই প্রথম সীমের ব্যবহার করেছিল। আর এটা হয়ে থাকে ব্যবহৃত মোবাইলের IMEI কোডের মাধ্যমে।

এই জন্যে পরিবর্তনের সময় মোবাইল ও সিম দুইটাই করতে হবে শুধু সিম পরিবর্তন যতেষ্ঠ নয়। সেই সাথে মেসেজিং এর জন্যে ইন্টারনেটের মাধ্যমেগুলো এবং নাম্বারের জন্যে Sudo, ONoff, Hushed, Text now ইত্যাদি যা বিদেশি নাম্বার দিয়ে থাকে সেসব ব্যবহার করা উচিত।

প্রশ্নঃ স্মার্ট ফোন বা ডিজিটাল ক্যামেরা দ্বারা ছবি তুলা এবং ইন্টারনেটে ছড়িয়ে দেওয়া কি বিপদজনক?

উত্তরঃ আমাদের এটি অবশ্যই মনে রাখতে হবে যে, আমাদের তুলা ছবিগুলো কিন্তু তার ভিতরের গোপনীয় তথ্য ও কোয়ালটির ডাটাকে সংরক্ষন করে রাখে। সেগুলো Exif Data নামে পরিচিত। উদাহরণস্বরূপ JPEG অথবা TIFF পিকচার এবং যেগুলো স্মার্ট ফোন বা ডিজিটাল ক্যামেরাগুলির মাধ্যমে তৈরি করা হয়, যেখানে অনেক তথ্য থাকে এবং সেই তথ্যগুলির মধ্যে রয়েছেঃ

(1) তারিখ ও ছবি তোলার সময়।

(2) ছবির (GPS) ভৌগোলিক অবস্থানের স্থানাঙ্ক।

(3) ক্যামেরা প্রকার, অ্যাপারচার, এবং ফোকাল দৈর্ঘ্য।

(4) অপারেটিং সিস্টেম, ফোন মডেল নম্বর এবং প্রস্তুতকারক।

আর একটা ভুল কাজ হচ্ছে, কতক ব্যবহারকারী ছবিগুলোতে কিছু Edit করে থাকে, যেমন ছবি কাটা এবং সেগুলোকে ইন্টারনেটে আপলোড করে। কিন্তু ছবি কাটা মূল ডাটাকে পরিবর্তন করে না বা সেটাকে ডিলিট করে না। তাই ছবির তথ্যকে পরিবর্তনের সফটওয়্যার ব্যবহারের পরামর্শ দিব। যেমনঃ Mat, Exif Tool, Fxiv2 ইত্যাদি।
নোটঃ স্ক্রীনশট GPS অবস্থানের তথ্য সংরক্ষন করে না। কিন্তু তারিখ, ও ছবি তোলার সময়, এবং ডিভাইস মডেল নম্বর অবশ্যই সেভ করে নেয়। তাই এগুলো বিষয়ে আমাদের সচেতন হওয়া একান্ত জরুরী।

প্রশ্নঃ ব্যক্তিগত ভার্চুওয়াল নেটওয়ার্ক ফ্রী (VPN) সেবা কি নিরাপত্তা বজায় রাখা এবং ট্র্যাকিং থেকে রক্ষা পাওয়ার জন্য উত্তম মাধ্যম?

উত্তরঃ অনেক দুর্ভাগ্যের বিষয় হলো ফ্রী VPN গুলো ব্যবহারকারীদেরকে বিভিন্ন রকমের বিপদে ঠেলে দেয়। তার মধ্য আছে তথ্য ও উপাত্ত চুরি করা অথবা ব্যবহারকারীদের ডাটা দিয়ে ব্যবসা করা ও সেগুলোকে ব্যবহারকারীর অগোচরেই বিজ্ঞাপণ সংস্থাগুলির নিকট বিক্রি করে দেওয়া। সুতরাং নিরাপত্তা বজায় রাখা ও ট্র্যাকিং থেকে রক্ষা পাওয়ার জন্য ফ্রী সেবা নেওয়ার ক্ষেত্রে উত্তম মাধ্যম হচ্ছে TOR নেটওয়ার্ক ব্যবহার করা।